ArubaOS-Switch, Comware and Cisco IOS CLI Reference Guide

Version 3.3

a Hewlett Packard Enterprise company

Table of Contents

Introduction 5
Revisions Status 7
Version 3.0 7
Version 3.1 7
Version 3.2 7
Version 3.3 7
Comware 5 and Comware 7 Integration 9
Using This Guide 11
Comware Differences 11
Navigation Differences Among CLIs 11
Configuration Differences Among CLIs 11
Terminology Differences 12
Disclaimer 12
Comparing View and Configuration Prompts 13
Comparing Frequently Used Commands 13
Chapter 1 Basic Switch Management 14
a) Management Access 14
b) Configuration Access 15
c) Console Access—Baud Rate 16
d) Console and Virtual Terminal Access—Timeout 17
e) Reload & Timed Reload 18
f) USB 23
g) System and Environment 24
h) Remote Management Sessions—Viewing 29
i) Remote Management Sessions—Terminating 32
j) Tech Support Information Output Listing 35
k) Filtering Output show running-config and display current-configuration 36
l) Motd 37
m) Source Interface for Management Communications 38
Chapter 2 Switch User ID and Password, and Console Access 42

a) Local User ID and Password, and console access 42
b) Recover Lost Password 56
c) Protect Local Password 58
d) Role based management 61
e) Password complexity 73
Chapter 3 Image or Operating System File Management 83
Chapter 4 Configuration File Management 99
Chapter 5 Syslog Services 116
Chapter 6 Time Service 123
a) NTP 123
b) SNTP 133
Chapter 7 SNMP 138
a) SNMP Version 1 and Version 2c 139
b) SNMP Version 3 152
Chapter 8 CLI Management Access – Telnet and SSH 164
a) Telnet 164
b) SSH 171
Chapter 9 GUI Management Access – HTTP and HTTPS 182
a) HTTP 182
b) HTTPS - SSL (Self-Signed Certificates) 187
Chapter 10 RADIUS Authentication for Switch Management 194
a) Basic Configuration 195
b) Privilege Mode 216
c) Commands Authorization 220
d) RADIUS Accounting 222
Chapter 11 TACACS+/HWTACACS Authentication for Switch Management 226
a) Basic Configuration 226
b) Privilege Mode 241
c) TACACS Accounting 244
Chapter 12 Discovery Protocols – LLDP and CDP 248
a) LLDP 248

b) CDP 255
Chapter 13 Out-of-Band Management 263
Chapter 14 Job Schedule 279
Chapter 15 Interface or Port Information and Nomenclature 287
Chapter 16 VLAN Management 304
a) Creating and Naming VLANs 304
b) Assigning Ports or Interfaces to VLANs 311
c) Assigning an IP Address to a VLAN 328
d) IP Helper to Relay / Forward DHCP Requests 330
Chapter 17 Advanced VLAN Features 336
a) Private VLAN 336
b) MVRP 353
c) VxLAN 360
d) MDNS, IPv6 ND snooping, BFD 363
e) RIPNG 364
f) IP-SLA, Portscan detection 365
g) Federal Govt Certification, Netdestination 370
Chapter 18 PoE (Power over Ethernet) 373
Chapter 19 VoIP Support 380
Chapter 20 Link Aggregation – LACP and Trunk 387
a) Link Aggregation Control Protocol (LACP) 387
b) Trunk 395
Chapter 21 RSTP 400
Chapter 22 MSTP 412
Chapter 23 PVST/PVST+/RPVST/RPVST+ 436
Chapter 24 RIP – v1 and v2 449
Chapter 25 OSPFv2 453
a) Single Area 453
b) Multiple Areas 456
c) Stub 458
d) Totally Stubby 459

e) Show or Display OSPF Commands 460
Chapter 26 BGP version 4 467
a) eBGP 468
b) iBGP 479
Chapter 27 VRRP 485
Chapter 28 ACLs 493
a) Definitions of Standard or Basic ACLs and Extended or Advanced ACLs 493
b) ACL Fundamental Configuration Options 494
Standard/Basic 494
Extended/Advanced 494
c) Routed/Layer 3 ACL (RACL) 504
Standard or Basic ACL 504
Extended or Advanced ACL 504
d) VLAN/Layer 2 Based ACL (VACL) 510
Standard or Basic ACL 510
Extended or Advanced ACL 510
e) Port ACL (PACL) 517
Standard or Basic ACL 517
Extended or Advanced ACL 517
Chapter 29 QoS 521
QoS Operational Characteristics 521
a) QoS 522
b) Rate Limiting 533
Chapter 30 IP Multicast 539
a) PIM Dense 540
b) PIM Sparse 543
c) IGMP 554
Chapter 31 Spanning Tree Hardening 556
a) UDLD and DLDP 558
b) BPDU Protection and BPDU Guard 562

c) Loop Protection 563
d) Root Guard 565
Chapter 32 DHCP Snooping 566
Chapter 33 ARP Protection, ARP Detection, and Dynamic ARP Inspection 575
Chapter 34 Connection Rate Filtering 584
Chapter 35 802.1X Authentication 590
a) 802.1X Authentication 590
b) MAC Authentication 611
c) Web or Portal Authentication 620
Chapter 36 Port Mirroring or Port Span 634
a) Local Mirror or SPAN 634
b) Remote Mirror or RSPAN 640
Chapter 37 Tunneled Node, Trust QoS, Clear Pass Intergration 647
Chapter 38 HP 3800 Stacking / HP IRF / Cisco Switch Stacks 651
Appendix A Comware Platforms – Default configuration 659
Appendix B Comware CLI Commands in ArubaOS-Switch Software 660
a) Fundamental Commands 660
b) Display Commands 662
Index 667

ArubaOS-Switch, Comware and Cisco IOS CLI Reference Guide

Introduction

Aruba designed this CLI Reference Guide to help Hewlett Packard Enterprise partners and customers who:

- Manage multi-vendor networks that include HPE and Cisco switches
- Have experience deploying Cisco switches and are now deploying HPE switches

This CLI Reference Guide compares many of the common commands in three switch operating systems: HPE ArubaOS-Switch (now the Aruba OS), HPE Comware version 5 and version 7, and Cisco IOS operating systems.

In this guide, we refer to HPE ProVision as ArubaOS-Switch, HPE Comware version 5 as Comware5, HPE Comware version 7 as Comware7, and Cisco IOS is referenced as Cisco.

The HPE ArubaOS-Switch operating system runs on 2530, 2920, 2930F, 3810M, 5400R, HPE 2620, HPE 3500, HPE 5400 and HPE 3800 switch platforms, where the image file starts with the letter "W". In addition, the HPE 3800 uses the same foundation ArubaOS-Switch operating system, but the image file starts with the letters "KA". The HPE 5400R zl2 also uses the same foundation ArubaOS-Switch operating system, but the image file starts with the letters "KB".

The HPE Comware5 operating system runs on HPE 12500, HPE 10500, HPE 7500, HPE 5920, HPE 5900, HPE 5830, HPE 5820, HPE 5800, HPE 5500 HI, HPE 5500 EI, HPE 5500 SI, HPE 4800G, HPE 3610, HPE 3600 EI, and HPE 3600SI switch platforms, and the HPE 8800, HPE 6600, HPE MSR50, HPE MSR30, HPE MSR20, HPE MSR20-1x, and HPE MSR900 router platforms.

The HPE Comware7 operating system runs on HPE FF 12900, HPE 12500, HPE 10500, HPE FF 7900, HPE 5930, HPE 5920, HEP 5900, HPE FF 5700, and HPE 5130 switch platforms, the HPE MSR2000 series router platforms, and the VSR100x series Virtual Services Router E-LTU.

The commands included in this guide were tested on the following:

- HPE 3800-24G-PoE+-2SFP+ switch running ArubaOS-Switch KA.16.03.0003
- HPE A5500-24G-PoE+ EI switch running Comware 5.20.99, Release 2221P07
- HPE 5900AF-48G-4XG-2QSFP+ switch running Comware 7.1.045, Release 2416
- Cisco WS-C3750E-24TD switch running Cisco IOS Software C3750E Software (C3750E-UNIVERSALK9-M), 15.0(1)SE

Additional HPE and Cisco switches and/or routers were used to provide systems connectivity and operational support as necessary. Likewise, various computers and Voice over IP (VoIP) phones were used to help test functionality and provide output for commands such as **show** or **display**.

Revisions Status

Version 3.0

Version 3.0 released in early 2015 and was a major update to include Comware 7.

Version 3.1

Version 3.1 released in late 2015 and included minor typographical changes.

Version 3.2

Version 3.2 released in mid-2016 and included the following content additions and changes:

- Title change to: Aruba HPE Networking and Cisco CLI Reference Guide
- New section in Chapter 2: d – Role Based Management
- New section in Chapter 2: e – Password Complexity
- Updates in Chapter 6: ArubaOS-Switch supports NTP
- New Chapter 13: Out-of-band management
- New Chapter 14: Job Schedule
- New Chapter 17: Advanced VLAN Capabilities

The commands included in Version 3.2 update were tested on the following:

- HP 3800-24G-PoE+-2SFP+ switch running ArubaOS-Switch KA.16.01.0007
- HP 5500-24G-PoE+ EI switch running Comware 5.20.99, Release 2221P25
- HP 5900AF-48G-4XG-2QSFP+ switch running Comware 7.1.045, Release 2422P01
- Cisco WS-C3750E-24TD switch running Cisco IOS Software C3750E Software (C3750E-UNIVERSALK9-M), 15.0(2)SE7

Version 3.3

Version 3.3 released in Feb-2017 and included the following content additions and changes:

- Title change to: ArubaOS-Switch, Comware and Cisco IOS CLI reference guide
- New enhancements in Chapter 2: d – Role Based Management
- New enhancements in Chapter 2: e – Password Complexity
- Updates in Chapter 6: ArubaOS-Switch supports NTP
- New updates in Chapter17: c: VxLAN
- New updates in Chapter17: d: MDNS, IPv6 ND Snooping, BFD
- New updates in Chapter17: e: RIPNG
- New updates in Chapter17: f: IP-SLA, Portscan Detection
- New updates in Chapter17: g: Federal Govt Certification, Netdestination
- New enhancements in Chapter 28: ACLs
- New chapter 37: Tunneled Node, Trust QoS, Clear Pass Integration

The commands included in Version 3.3 update were tested on the following:

- HP 3800-24G-PoE+-2SFP+ switch running ArubaOS-Switch KA.16.03.0003

Comware 5 and Comware 7 Integration

In order to preserve the 3-column format of the document for legability, Comware7 has been integrated with Comware5 into a single column. The following details the three options of this integration:

1. Where Comware5 & Comware7 have the same commands and same options within commands the Comware box color is dark blue and is depicted as Comware:

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# console inactivity-timer ?	[Comware]user-interface aux 0	Cisco(config)#line console 0

2. Where Comware5 & Comware7 have same commands, but different options within commands, the commands section box is dark blue and depicted as Comware, the command details section has Comware5 box in dark blue and the Comware7 box in green:

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch# show tech	<Comware>display diagnostic-information	Cisco#show tech-support

Comware5

```
<Comware5>display diagnostic-information ?
  |     Matching output
  <cr>

<Comware5>display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:
```

Comware7

```
<Comware7>display diagnostic-information ?
  STRING          [drive][path][file name]
  flash:          Device name
  hardware        Hardware information for diagnosis
  infrastructure  Infrastructure information for diagnosis
  l2              L2 information for diagnosis
  l3              L3 information for diagnosis
  service         Service information for diagnosis
  slot1#flash:    Device name
  slot1#usba0:    Device name
  usba0:          Device name
  <cr>


<Comware7>display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:
```

3. Where Comware5 & Comware7 have different commands and command options, Comware5 commands and command details section boxes are dark blue and Comware7 commands and command details section boxes are green:

ArubaOS-Switch	Comware5	Cisco
ArubaOS-Switch(config)# lldp run	[Comware5]lldp enable	Cisco(config)#lldp run
	Comware7	
	[Comware7]lldp global enable	
ArubaOS-Switch(config)#aaa port-access use-lldp-data		Cisco(config)#enable lldp service
ArubaOS-Switch(config)#no aaa port-access use-lldp-data		Cisco(config)#disable lldp service
ArubaOS-Switch(config)#lldp config <port_num> basicTlvEnable management_addr		

Comware5

```
[Comware5]lldp ?
  compliance        Enable compliance with another link layer discovery protocol
  enable            Enable capability
  fast-count        The fast-start times of transmitting frames
  hold-multiplier   Hold multiplicator for TTL
  timer             Timer of LLDP

[Comware5]lldp enable ?
  <cr>

[Comware5]lldp enable
```

Comware7

```
[Comware7]lldp ?
  compliance        Enable compliance with another link layer discovery protocol
  fast-count        The fast-start times of transmitting frames
  global            Specify global
  hold-multiplier   Hold multiplicator for TTL
  max-credit        Specify LLDP maximum transmit credit
  mode              Specify LLDP bridge mode
  timer             Timer of LLDP

[Comware7]lldp global ?
  enable  Enable capability

[Comware7]lldp global enable ?
  <cr>

[Comware7]lldp global enable
```

Using This Guide

This CLI Reference Guide provides CLI command comparisons in two different formats:

- Side-by-side comparison—It provides a table of the basic commands required to execute a given function in each of the operating systems. In this side-by-side comparison, each platform's commands do not always start at the top of the column. Instead, commands that have similar functions are aligned side by side so that you can easily "translate" the commands on one platform with similar commands on another platform.
- Detailed comparison—Beneath the side-by-side comparison, this guide provides a more in-depth comparison, displaying the output of the command and options.

Occasionally, there are few, if any, similarities among the commands required to execute a function or feature in each operating system. In these instances, each column has the commands necessary to implement the specific function or feature, and the side-by-side comparison does not apply.

Comware Differences

If you are familiar with either the HPE ArubaOS-Switch CLI or the Cisco IOS CLI, you will notice that the Comware CLI is organized slightly differently. Comware was designed for Internet service providers (ISPs). Many features and functions—such as security and Quality of Service (QoS)—are multi-tiered to support the different needs of multiple entities accessing the same switch.

Navigation Differences Among CLIs

Basic CLI navigation on all three platforms is very similar, with one notable difference:

- With ArubaOS-Switch, you can use the **Tab** key for command completion; you can also use the **Tab** key or the **?** key to find more command options. In addition, typing "help" at the end of a command may provide additional descriptive information about the command.
- With Comware or Cisco, you can use the **Tab** key for command completion, but you use the **?** key to find more command options.

Configuration Differences Among CLIs

For interface IP addressing and interface-specific routing protocol configuration, you execute most commands differently depending on the platform:

- On ArubaOS-Switch, you configure the aforementioned components in a VLAN context.
- On Comware or Cisco, you configure the aforementioned components in an interface (VLAN for switch) context.

Terminology Differences

Among the three operating systems, there are some differences in the terms used to describe features. The table below lists three such terms that could be confusing.

In Cisco and Comware, for example, the term *trunk* refers to an interface that you configure to support 802.1Q VLAN tagged frames. That is, an interface that you configure to support multiple VLANs is a *trunk* interface in each VLAN in Cisco and Comware. In the ArubaOS-Switch operating system, an interface that supports multiple VLANs is a *tagged* interface in each VLAN.

In addition, ArubaOS-Switch refers to aggregated interfaces as a *trunk*. In Comware the term is *bridge aggregation*, while in Cisco it is *EtherChannel*.

Interface use	ArubaOS-Switch	Comware	Cisco
Non-802.1Q interfaces (such as used for computers or printers)	`untagged`	`access`	`access`
802.1Q interfaces (such as used for switch-to-switch, switch-to-server, and switch-to-VoIP phones)	`tagged`	`trunk` (Note: some display views will denote tagged)	`trunk`
Aggregated interfaces	`trunk`	`bridge aggregation`	`etherchannel`

Disclaimer

Although Aruba conducted extensive testing to create this guide, it is impossible to test every conceivable configuration and scenario. Do not assume, therefore, that this document is complete for every environment or each manufacturer's complete product platforms and software versions. For complete and detailed information on all commands and their options, refer to each manufacturer's documentation accordingly.

Comparing View and Configuration Prompts

The table below compares the differences in each system's display for view and configuration prompts.

Context Legend	ArubaOS-Switch	Comware	Cisco
U = User Exec / User View	ArubaOS-Switch>	<Comware>	Cisco>
P = Privileged Exec	ArubaOS-Switch#		Cisco#
S = System View (equal to Priviledged Exec)		[Comware]	
C = Configuration	ArubaOS-Switch(config)#	[Comware]	Cisco(config)#

Comparing Frequently Used Commands

The table below lists frequently used commands for each operating system.

	ArubaOS-Switch		Comware		Cisco
U	enable	U	system-view	U	enable
P	configure	U	system-view (configuration mode is same as being at System View)	U	configure terminal
U/P/C	show flash	U	dir	U/P	show flash
U/P/C	show version	U/S	display version	U/P	show version
P/C	show run	U/S	display current-configuration	P	show run
P/C	show config	U/S	display saved-configuration	P	show start
U/P/C	show history	U/S	display history	U/P	show history
U/P/C	show logging	U/S	display info-center	U/P	show logging
U/P/C	show ip route	U/S	display ip routing-table	U/P	show ip route
U/P/C	show ip	U/S	display ip interface brief	U/P	show ip interface brief
U/P/C	show interface brief	U/S	display interface brief	U/P	show interfaces status
P/C	erase startup-config	U	reset saved	P	erase start
P/C	show config <filename>	U	more <filename>	P	more flash:/<filename>
P/C	reload	U	reboot	P	reload
P/C	write memory	U/S	save	P	write memory
P	show tech	U/S	display diagnostic-information	U/P	show tech-support
U/P/C	show	U/S	display	U/P	show
U/P/C	no	U/S	undo	P	no
C	end	S	return	C	end
U/P/C	exit	U/S	quit	U/P/C	exit
P/C	erase	U/S	delete	P	erase
P/C	copy	U	copy/tftp	P	copy
C	hostname	S	sysname	C	hostname
C	logging	S	info-center	C	logging
C	router rip	S	rip	C	router rip
C	router ospf	S	ospf	C	router ospf
C	ip route	S	ip route-static	C	ip route
C	access-list	S	acl	C	access-list

Chapter 1 Basic Switch Management

This chapter compares commands primarily used for device navigation, device information, and device management.

- Management access
- Configuration access
- Console access
- Switch reload
- USB
- System and environment
- Remote management sessions (viewing and terminating)
- Tech support output
- Filtering output of **show running-config** and **display current-configuration** commands
- Motd
- Source interface for management communications

a) Management Access

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch> enable	<Comware> system-view System View: return to User View with Ctrl+Z.	Cisco> enable
ArubaOS-Switch#	[Comware]	Cisco#

ArubaOS-Switch

```
ArubaOS-Switch> enable

ArubaOS-Switch#
```

Comware

```
<Comware> system-view
System View: return to User View with Ctrl+Z.

[Comware]
```

Cisco

```
Cisco> enable

Cisco#
```

b) Configuration Access

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch# configure	No specific command, see note below	Cisco# configure terminal Enter configuration commands, one per line. End with CNTL/Z.
ArubaOS-Switch(config)#	[Comware]	Cisco(config)#

ArubaOS-Switch

```
ArubaOS-Switch# configure ?
 terminal              Optional keyword of the configure command.
 <cr>

ArubaOS-Switch# configure

ArubaOS-Switch(config)#
```

Comware

Comware does not have a specific configuration mode, when at "System View" context, configuration commands are entered directly at that prompt.

When you are configuring interfaces, protocols, and so on, the prompt will change to indicate that sub-level.

```
<Comware> system-view

[Comware]
```

Cisco

```
Cisco# configure ?
  confirm            Confirm replacement of running-config with a new config
                     file
  memory             Configure from NV memory
  network            Configure from a TFTP network host
  overwrite-network  Overwrite NV memory from TFTP network host
  replace            Replace the running-config with a new config file
  revert             Parameters for reverting the configuration
  terminal           Configure from the terminal
  <cr>

Cisco#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Cisco(config)#
```

c) Console Access—Baud Rate

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# console baud-rate ?	[Comware]user-interface aux 0 [Comware-ui-aux0]speed ?	Cisco(config)#line console 0 Cisco(config-line)#speed ?

ArubaOS-Switch

```
ArubaOS-Switch(config)# console baud-rate ?
 speed-sense      (this is the default configuration setting)
 1200
 2400
 4800
 9600
 19200
 38400
 57600
 115200

ArubaOS-Switch(config)# console baud-rate 9600
This command will take effect after saving the configuration and
rebooting the system.

ArubaOS-Switch(config)#
```

Comware

Note:

9600 is the default configuration setting for H3C labeled devices.

19200 is the default configuration setting for 3Com labeled devices. However, after executing the 'brand hp' command, the default speed is now 9600, see Appendix A for additional information.

```
[Comware]user-interface aux 0

[Comware-ui-aux0]speed ?
  300      Only async serial user terminal interface can be configured
  600      Only async serial user terminal interface can be configured
  1200     Only async serial user terminal interface can be configured
  2400     Only async serial user terminal interface can be configured
  4800     Only async serial user terminal interface can be configured
  9600     Only async serial user terminal interface can be configured
  19200    Only async serial user terminal interface can be configured
  38400    Only async serial user terminal interface can be configured
  57600    Only async serial user terminal interface can be configured
  115200   Only async serial user terminal interface can be configured

[Comware-ui-aux0]speed 9600 ?
  <cr>

[Comware-ui-aux0]speed 9600

[Comware-ui-aux0]
```

Cisco

```
Cisco(config)#line console 0

Cisco(config-line)#speed ?
  <0-4294967295>  Transmit and receive speeds  (9600 is the default configuration setting)

Cisco(config-line)#speed 9600

Cisco(config-line)#
```

d) Console and Virtual Terminal Access—Timeout

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# console inactivity-timer ?	[Comware]user-interface aux 0	Cisco(config)#line console 0
	[Comware-ui-aux0]idle-timeout ?	Cisco(config-line)#exec-timeout ?
	[also]	[also]
	[Comware]user-interface vty 0	Cisco(config)#line vty 0
	[Comware-ui-vty0]idle-timeout ?	Cisco(config-line)#exec-timeout ?
Note: console inactivity-timer works for telnet and ssh sessions as well.		

ArubaOS-Switch

```
ArubaOS-Switch(config)# console inactivity-timer ?
<0-120>                Enter an integer number.
                        (0 is the default configuration setting)

ArubaOS-Switch(config)# console inactivity-timer 120

ArubaOS-Switch(config)#
```

Note: console inactivity-timer works for telnet and ssh sessions as well.

Comware

```
[Comware]user-interface aux 0

[Comware-ui-aux0]idle-timeout ?
  INTEGER<0-35791>  Specify the idle timeout in minutes for login user.
                     (10 is the default configuration setting)

[Comware-ui-aux0]idle-timeout 20 ?
  INTEGER<0-59>  Specify the idle timeout in seconds for login user.
  <cr>
                     (0 is the default configuration setting)

[Comware-ui-aux0]idle-timeout 20 10

[Comware-ui-aux0]
```

[also]

```
[Comware]user-interface vty 0

[Comware-ui-vty0]idle-timeout 20 10
```

Cisco

```
Cisco(config)#line console 0

Cisco(config-line)#exec-timeout ?
  <0-35791>  Timeout in minutes
                     (10 is the default configuration setting)

Cisco(config-line)#exec-timeout 20 ?
  <0-2147483>  Timeout in seconds
                     (0 is the default configuration setting)

Cisco(config-line)#exec-timeout 20 10

Cisco(config-line)#
```

[also]

```
Cisco(config)#line vty 0

Cisco(config-line)#exec-timeout 20 10
```

e) Reload & Timed Reload

ArubaOS-Switch	Comware5	Cisco
ArubaOS-Switch# reload	<Comware5>reboot	Cisco#reload
ArubaOS-Switch# reload ?	<Comware5>reboot ?	Cisco#reload ?
	<Comware5>schedule reboot ?	
ArubaOS-Switch# show reload ?	<Comware5>display schedule reboot	Cisco#show reload
ArubaOS-Switch(config)# no reload	<Comware5>undo schedule reboot	Cisco#reload cancel
	Comware7	
	<Comware7>reboot	
	<Comware7>reboot ?	
	<Comware7>scheduler reboot ?	
	<Comware7>display scheduler ?	
	<Comware7>undo scheduler reboot	

ArubaOS-Switch

```
ArubaOS-Switch# reload
System will be rebooted from primary image. Do you want to continue [y/n]?
```

[for timed reboot]

```
ArubaOS-Switch# reload ?
```

```
 after                  Warm reboot in a specified amount of time.
 at                     Warm reboot at a specified time; If the mm/dd/yy is left blank,
                        the current day is assumed.
 <cr>

ArubaOS-Switch# reload at ?
 HH:MM[:SS]             Time on given date to do a warm reboot.

ArubaOS-Switch# reload at 23:00 ?
 MM/DD[/[YY]YY]         Date on which a warm reboot is to occur.
 <cr>

ArubaOS-Switch# reload at 23:00 03/04/2015 ?
 <cr>

ArubaOS-Switch# reload at 23:00 03/04/2015
    Reload scheduled at 23:00:13 03/04/2015
                  (in 0 days, 23 hours, 12 minutes)
System will be rebooted at the scheduled time from primary image.
Do you want to continue [y/n]?  y
ArubaOS-Switch#
```

-or-

```
ArubaOS-Switch# reload after
 [[DD:]HH:]MM           Enter a time.



ArubaOS-Switch# show reload ?
 after                  Shows the time until a warm reboot is scheduled.
 at                     Shows the time and date a warm reboot is scheduled.

ArubaOS-Switch# show reload after
    Reload scheduled for 23:00:57 03/04/2015
               (in 0 days, 23 hours, 9 minutes)


ArubaOS-Switch(config)# no reload

ArubaOS-Switch(config)# show reload after
    reload is not scheduled
```

Comware5

```
<Comware5>reboot ?
  slot  Specify the slot number
  <cr>

<Comware5>reboot

-or-

<Comware5>reboot slot ?
  INTEGER<1>  Slot number

<Comware5>reboot slot 1 ?
  <cr>
```

[for timed reboot]

```
<Comware5>schedule reboot ?
  at     Specify the exact time
```

```
  delay  Specify the time interval

<Comware5>schedule reboot at ?
  STRING  Exact time(hh:mm)

<Comware5>schedule reboot at 23:00 ?
  DATE  Date to reboot (mm/dd/yyyy or yyyy/mm/dd)
  <cr>

<Comware5>schedule reboot at 23:00 03/04/2015 ?
  <cr>

<Comware5>schedule reboot at 23:00 03/04/2015
Reboot system at 23:00 03/04/2015(in 23 hour(s) and 14 minute(s)). confirm? [Y/N]:y
<Comware5>
%Mar  3 23:45:24:781 2015 Comware5 CMD/5/CMD_REBOOT_SCHEDULED: aux0 set schedule reboot
parameters at 23:45:24 03/03/2015, and system will reboot at 23:00 03/04/2015.
<Comware5>
```

-or-

```
<Comware5>schedule reboot delay ?
  STRING  Time interval(mm or hh:mm)

<Comware5>schedule reboot delay 30 ?
  <cr>

<Comware5>schedule reboot delay 30
Reboot system at 15:43 03/03/2015(in 0 hour(s) and 30 minute(s)). confirm? [Y/N]:y
<Comware5>
%Mar  3 15:13:55:852 2015 Comware5 CMD/5/CMD_REBOOT_SCHEDULED: aux0 set schedule reboot
parameters at 15:13:55 03/03/2015, and system will reboot at 15:43 03/03/2015.


<Comware5>display schedule reboot
System will reboot at 23:00 03/04/2015 (in 22 hours and 58 minutes).


<Comware5>undo schedule reboot
<Comware5>
%Mar  3 23:45:36:426 2015 Comware5 CMD/5/CMD_REBOOT_CANCEL: aux0 cancelled reboot parameters
at 23:45:36 03/03/2015.
```

Comware7

```
<Comware7>reboot ?
  force  Forcibly reboot without checking
  slot   Specify the slot number
  <cr>

<Comware7>reboot
```

-or-

```
<Comware7>reboot force ?
  <cr>

<Comware7>reboot force

<Comware7>reboot slot ?
  <1>  Slot number

<Comware7>reboot slot 1 ?
```

```
  force    Forcibly reboot without checking
  subslot  Specify the subslot number
  <cr>

<Comware7>reboot slot 1
```

[for timed reboot]

```
<Comware7>scheduler reboot ?
  at     Specify the execution time
  delay  Specify the delay time

<Comware7>scheduler reboot at ?
  TIME  Execution time (HH:MM)

<Comware7>scheduler reboot at 23:00 ?
  DATE  Execution date (MM/DD/YYYY or YYYY/MM/DD)
  <cr>

<Comware7>scheduler reboot at 23:00 03/09/2015 ?
  <cr>

<Comware7>scheduler reboot at 23:00 03/09/2015
Reboot system at 23:00:00 03/09/2015(in 7 hours and 51 minutes). Confirm?[Y/N]:y
<Comware7>%Mar  9 15:08:34:699 2015 Comware7 SCH/5/SCH_REBOOT_SCHEDULED: aux0 set schedule
reboot parameters at 15:08:30 03/09/2015, and system will reboot at 23:00:00 03/09/2015.

<Comware7>
```

-or-

```
<Comware7>scheduler reboot delay ?
  STRING<1-6>  Interval (HH:MM or MM)

<Comware7>scheduler reboot delay 07:45 ?
  <cr>

<Comware7>scheduler reboot delay 07:45
Reboot system at 22:56:01 03/09/2015(in 7 hours and 45 minutes). Confirm?[Y/N]:y
<Comware7>%Mar  9 15:11:04:975 2015 Comware7 SCH/5/SCH_REBOOT_SCHEDULED: aux0 set schedule
reboot parameters at 15:11:01 03/09/2015, and system will reboot at 22:56:01 03/09/2015.


<Comware7>display scheduler reboot
System will reboot at 23:00:00 03/09/2015(in 7 hours and 47 minutes).


<Comware7>undo schedule reboot
<Comware7>%Mar  9 15:09:23:490 2015 Comware7 SCH/5/SCH_REBOOT_CANCEL: aux0 cancelled reboot
parameters at 15:09:23 03/09/2015.
```

Cisco

```
Cisco#reload
Proceed with reload? [confirm]
```

[for timed reboot]

```
Cisco#reload ?
  /noverify  Don't verify file signature before reload.
  /verify    Verify file signature before reload.
  LINE       Reason for reload
  at         Reload at a specific time/date
  cancel     Cancel pending reload
  in         Reload after a time interval
  slot         Slot number card
  standby-cpu  Standby RP
  <cr>

Cisco#reload at ?
  hh:mm  Time to reload (hh:mm)

Cisco#reload at 23:00 ?
  <1-31>  Day of the month
  LINE    Reason for reload
  MONTH   Month of the year
  <cr>

Cisco#reload at 23:00 march ?
  <1-31>  Day of the month

Cisco#reload at 23:00 march 5 ?
  LINE  Reason for reload
  <cr>

Cisco#reload at 23:00 march 5

System configuration has been modified. Save? [yes/no]: y
Building configuration...
[OK]
Reload scheduled for 23:00:00 central Thu Mar 5 2015 (in 22 hours and 16 minutes) by console
Proceed with reload? [confirm]
Cisco#
Mar  5 06:43:40.282: %SYS-5-SCHEDULED_RELOAD: Reload requested for 23:00:00 central Thu Mar
5 2015 at 00:43:27 central Thu Mar 5 2015 by console.
Cisco#
```

-or-

```
Cisco#reload in ?
Delay before reload (mmm or hhh:mm)

Cisco#reload in 23:10 ?
  LINE  Reason for reload
  <cr>



Cisco#show reload
Reload scheduled for 23:00:00 central Thu Mar 5 2015 (in 22 hours and 15 minutes) by console

Cisco#reload cancel
Cisco#
```

```
***
*** --- SHUTDOWN ABORTED ---
***

Mar  5 06:45:38.016: %SYS-5-SCHEDULED_RELOAD_CANCELLED:  Scheduled reload cancelled at
00:45:38 central Thu Mar 5 2015
```

f) USB

ArubaOS-Switch	Comware5	Cisco
	not an available feature	not an available feature
	Comware7	
ArubaOS-Switch# dir	<Comware7>dir usba0:/	
ArubaOS-Switch# show usb-port	<Comware7>display device usb	

ArubaOS-Switch

```
ArubaOS-Switch# dir ?
 PATHNAME-STR          Display a list of the files and subdirectories in a directory on a
                       USB device.
 <cr>

ArubaOS-Switch# dir

Listing Directory /ufa0:
-rwxrwxrwx   1   16719093 Nov 19 15:21 K_15_16_0005.swi
-rwxrwxrwx   1   16208437 Sep 11 19:10 K_15_15_0008.swi
-rwxrwxrwx   1        849 Mar 03 17:52 ArubaOS-Switch-config.cfg


ArubaOS-Switch# show usb-port

 USB port status: enabled
 USB port power status: power on      (USB device detected in port)
```

Comware5

not an available feature

Comware7

```
<Comware7>display device usb ?
  >        Redirect it to a file
  >>       Redirect it to a file in append mode
  slot     Specify the slot number
  verbose  Display detailed information
  |        Matching output
  <cr>

<Comware7>display device usb
slot 1:
      Device Name :   usba
      State       : Normal

<Comware7>dir usba0:/
Directory of usba0:
```

```
   0 -rw-     7309312 Mar 23 2015 15:04:02   5900_5920-cmw710-boot-r2311p05.bin
   1 -rw-    10986496 Mar 23 2015 15:08:32   5900_5920-cmw710-boot-r2416.bin
   2 -rw-    54262784 Mar 23 2015 15:07:08   5900_5920-cmw710-system-r2311p05.bin
   3 -rw-    66350080 Mar 23 2015 15:13:04   5900_5920-cmw710-system-r2416.bin
   4 -rw-        5429 Mar 23 2015 14:43:04   test.cfg

984816 KB total (699456 KB free)
```

Cisco

not an available feature

g) System and Environment

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch# show system information ArubaOS-Switch# show modules	<Comware>display device manuinfo <Comware>display device verbose	Cisco#show inventory Cisco#show version
ArubaOS-Switch# show system fans	<Comware>display fan	Cisco#show env fan
ArubaOS-Switch# show system power-supply	<Comware>display power	Cisco#show env power
ArubaOS-Switch# show system temperature	<Comware>display environment	Cisco#show env temperature
ArubaOS-Switch(config)#Allow-v2-modules erase		
ArubaOS-Switch(config)#Show running-config v3-specific		

ArubaOS-Switch

```
ArubaOS-Switch# show system ?
 chassislocate         Show information about the Locator LED.
 fans                  Show system fan status.
 information           Show global configured and operational system parameters.If
                       stacking is enabled it shows system information of all the stack
                       members.
 power-consumption     Show switch blade power consumption information.
 power-supply          Show Chassis Power Supply info and settings.If stacking is
                       enabled, shows power supply info and settings of all the stack
                       members.
 temperature           Show current temperature sensor information.
 <cr>

ArubaOS-Switch# show system information

 Status and Counters - General System Information

  System Name        : ArubaOS-Switch
  System Contact     :
  System Location    :

  MAC Age Time (sec) : 300
```

```
  Time Zone          : -360
  Daylight Time Rule : Continental-US-and-Canada

  Software revision  : KA.15.16.0005        Base MAC Addr      : 009c02-d53980
  ROM Version        : KA.15.09             Serial Number      : xxxxxxxxxx

  Up Time            : 34 mins              Memory   - Total   : 795,353,088
  CPU Util (%)       : 0                               Free    : 665,924,808

  IP Mgmt  - Pkts Rx : 199                  Packet   - Total   : 6750
             Pkts Tx : 220                  Buffers    Free    : 4830
                                                       Lowest  : 4810
                                                       Missed  : 0

ArubaOS-Switch# show modules
Status and Counters - Module Information

  Chassis: 3800-24G-PoE+-2SFP+  J9573A         Serial Number:   xxxxxxxxxx


  Slot     Module Description                        Serial Number    Status
  -------- ----------------------------------------- ---------------- --------





ArubaOS-Switch# show system fans

Fan Information
  Num  | State       | Failures
-------+-------------+----------
Fan-1  | Fan OK      |   0
Fan-2  | Fan OK      |   0
Fan-3  | Fan OK      |   0
Fan-4  | Fan OK      |   0

0 / 4 Fans in Failure State
0 / 4 Fans have been in Failure State

ArubaOS-Switch# show system power-supply

Power Supply Status:

 PS#     Model        State         AC/DC  + V      Wattage   Max
 ----- --------- --------------- ----------------- --------- ------
 1     J9580A    Powered           AC 120V/240V       71    1000
 2     Unknwn    Not Present                           0       0


   1 /  2 supply bays delivering power.
   Currently supplying 71 W / 1000 W total power.



ArubaOS-Switch# show system temperature

System Air Temperature
  Temp    Current  Max   Min
  Sensor  Temp     Temp  Temp  Threshold  OverTemp
  ------- -------- ----- ----- ---------- ---------
  Chassis 28C      28C   0C    55C        NO
```

Comware

```
<Comware>display device ?
  chassis   Specify the chassis number
  manuinfo  Manufacture information
  slot      Specify the slot number
  verbose   Display detail information
  |         Matching output
  <cr>

<Comware>display device manuinfo ?
  slot  Specify the slot number
  |     Matching output
  <cr>

<Comware>display device manuinfo
Slot 1:
DEVICE_NAME          : S5500-28C-PWR-EI
DEVICE_SERIAL_NUMBER : xxxxxxxxxxxx
MAC_ADDRESS          : 0023-89D5-A059
MANUFACTURING_DATE   : 2010-02-16
VENDOR_NAME          : H3C


<Comware>display device verbose ?
  |     Matching output
  <cr>


<Comware>display device verbose
 Slot 1
SubSNo PortNum PCBVer FPGAVer CPLDVer BootRomVer AddrLM Type       State
0      28      REV.C  NULL    002     710        IVL    MAIN       Normal

slot 1 info:
Up Time     : 0 weeks, 0 days, 1 hours, 22 minutes
Brd Type    : HP A5500-24G-PoE+ EI Switch with 2 Interface Slots
Brd Status  : Master
Sft Ver     : Release 2221P07
Patch Ver   : None
PCB Ver     : REV.C
BootRom Ver : 721
CPLD Ver    : 002


<Comware>display fan ?
  slot  Display slot ID
  |     Matching output
  <cr>

<Comware>display fan
 Slot 1
      FAN    1
      State    : Normal


<Comware>display power ?
  slot  Display slot ID
  |     Matching output
  <cr>

<Comware>display power
 Slot 1
```

```
      Power    1
      State    : Normal
      Type     : AC


<Comware>display environment ?
  slot  Specify the slot number
  |     Matching output
  <cr>

<Comware>display environment
Slot 1
System temperature information (degree centigrade):
-----------------------------------------------------------------------------
Sensor     Temperature  LowerLimit  WarningLimit  AlarmLimit ShutdownLimit
hotspot 1  33           -5          55            NA          NA
```

Cisco

```
Cisco#show inventory
NAME: "1", DESCR: "WS-C3750E-24TD"
PID: WS-C3750E-24TD-S  , VID: V02  , SN: xxxxxxxxxxx

NAME: "Switch 1 - Power Supply 0", DESCR: "FRU Power Supply"
PID: C3K-PWR-265WAC    , VID: V01Q , SN: xxxxxxxxxxx

Cisco#show version
Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Version 15.0(1)SE, RELEASE
SOFTWARE (fc1)
...
Cisco uptime is 1 hour, 9 minutes
System returned to ROM by power-on
System restarted at 23:56:02 central Wed Mar 4 2015
System image file is "flash:c3750e-universalk9-mz.150-1.SE.bin"
...
cisco WS-C3750E-24TD (PowerPC405) processor (revision F0) with 262144K bytes of memory.
Processor board ID FDO1231V0US
Last reset from power-on
1 Virtual Ethernet interface
1 FastEthernet interface
28 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:22:91:AB:43:80
Motherboard assembly number     : 73-10313-11
Motherboard serial number       : xxxxxxxxxxx
Model revision number           : F0
Motherboard revision number     : A0
Model number                    : WS-C3750E-24TD-S
Daughterboard assembly number   : 800-28590-01
Daughterboard serial number     : xxxxxxxxxxx
System serial number            : xxxxxxxxxxx
Top Assembly Part Number        : 800-27546-03
Top Assembly Revision Number    : A0
Version ID                      : V02
CLEI Code Number                : xxxxxxxxxxx
Hardware Board Revision Number  : 0x01


Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
```

```
*    1 30    WS-C3750E-24TD     15.0(1)SE             C3750E-UNIVERSALK9-M


Cisco#sh env ?
  all          Show all environment status
  fan          Show fan status
  power        Show power supply status
  rps          Show RPS status
  stack        Show Stack-wide all environment status
  temperature  Show temperature status
  xps          Show XPS status

Cisco#show env fan
FAN is OK





Cisco#sh env power ?
  all     All power supplies
  switch  Switch number
  |       Output modifiers
  <cr>

Cisco#show env power
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--- ------------------  ----------  ---------------  -------  -------  -----
 1  C3K-PWR-265WAC      xxxxxxxxxxx OK               Good     N/A      265/0

Cisco#show env temperature ?
  status  Show Temperature status and threshold values
  |       Output modifiers
  <cr>

Cisco#show env temperature
SYSTEM TEMPERATURE is OK
```

h) Remote Management Sessions—Viewing

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch# show telnet	<Comware>display users	Cisco# show users

ArubaOS-Switch

```
ArubaOS-Switch# show telnet ?
 <cr>

ArubaOS-Switch# show telnet

 Telnet Activity

 Source IP Selection: Outgoing Interface

 -------------------------------------------------------
 Session  : **  1
 Privilege: Manager
 From     : Console
 To       :
 -------------------------------------------------------
 Session  :     2
 Privilege: Manager
 From     : 10.0.100.87
 To       :
 -------------------------------------------------------
 Session  :     3
 Privilege: Manager
 From     : 10.0.100.84
 To       :
```

Comware5

```
<Comware5> display users ?
  all   The information of all user terminal interfaces
  |     Matching output
  <cr>

<Comware5> display users
The user application information of the user interface(s):
  Idx UI      Delay    Type Userlevel
F 0   AUX 0   00:00:00      3
  25  VTY 0   00:00:05 TEL  3
  26  VTY 1   00:02:32 TEL  3

Following are more details.
VTY 0   :
        Location: 10.0.100.84
VTY 1   :
        Location: 10.0.100.87
 +    : Current operation user.
 F    : Current operation user work in async mode.


<Comware5>dis users all ?
  |     Matching output
  <cr>

<Comware5> display users all
The user application information of all user interfaces:
  Idx UI      Delay    Type Userlevel
F 0   AUX 0   00:00:00      3
```

```
+ 25  VTY 0   00:01:05 TEL  3
+ 26  VTY 1   00:03:32 TEL  3
  27  VTY 2
  28  VTY 3
  29  VTY 4
  30  VTY 5
  31  VTY 6
  32  VTY 7
  33  VTY 8
  34  VTY 9
  35  VTY 10
  36  VTY 11
  37  VTY 12
  38  VTY 13
  39  VTY 14
  40  VTY 15

Following are more details.
VTY 0   :
        Location: 10.0.100.84
VTY 1   :
        Location: 10.0.100.87
 +    : User-interface is active.
 F    : User-interface is active and work in async mode.
```

Comware7

```
<Comware7>display users  ?
  >     Redirect it to a file
  >>    Redirect it to a file in append mode
  all   Information about all lines
  |     Matching output
  <cr>

<Comware7>display users
  Idx  Line    Idle       Time              Pid     Type
F 0    AUX 0   00:00:00   Mar 23 15:22:58   538
  129  VTY 0   00:02:10   Mar 23 15:41:18   613     TEL
  130  VTY 1   00:01:39   Mar 23 15:45:49   621     TEL

Following are more details.
VTY 0   :
        Location: 10.0.100.84
VTY 1   :
        Location: 10.1.1.108
 +    : Current operation user.
 F    : Current operation user works in async mode.

<Comware7>display users all ?
  >     Redirect it to a file
  >>    Redirect it to a file in append mode
  |     Matching output
  <cr>

<Comware7>display users all
  Idx  Line    Idle       Time              Pid     Type
F 0    AUX 0   00:00:00   Mar 23 15:22:58   538
+ 129  VTY 0   00:02:52   Mar 23 15:41:18   613     TEL
+ 130  VTY 1   00:02:21   Mar 23 15:45:49   621     TEL
  131  VTY 2
  132  VTY 3
  133  VTY 4
  134  VTY 5
  135  VTY 6
```

```
  136  VTY 7
  137  VTY 8
  138  VTY 9
  139  VTY 10
  140  VTY 11
  141  VTY 12
  142  VTY 13
  143  VTY 14
  144  VTY 15
  145  VTY 16
  146  VTY 17
  147  VTY 18
  148  VTY 19
  149  VTY 20
  150  VTY 21
  151  VTY 22
  152  VTY 23
  153  VTY 24
  154  VTY 25
  155  VTY 26
  156  VTY 27
  157  VTY 28
  158  VTY 29
  159  VTY 30
  160  VTY 31
  161  VTY 32
  162  VTY 33
  163  VTY 34
  164  VTY 35
  165  VTY 36
  166  VTY 37
  167  VTY 38
  168  VTY 39
  169  VTY 40
  170  VTY 41
  171  VTY 42
  172  VTY 43
  173  VTY 44
  174  VTY 45
  175  VTY 46
  176  VTY 47
  177  VTY 48
  178  VTY 49
  179  VTY 50
  180  VTY 51
  181  VTY 52
  182  VTY 53
  183  VTY 54
  184  VTY 55
  185  VTY 56
  186  VTY 57
  187  VTY 58
  188  VTY 59
  189  VTY 60
  190  VTY 61
  191  VTY 62
  192  VTY 63

Following are more details.
VTY 0   :
        Location: 10.0.100.84
VTY 1   :
        Location: 10.1.1.108
```

```
 +     : Line is active.
 F     : Line is active and works in async mode.
```

Cisco

```
Cisco#show users ?
  all   Include information about inactive ports
  wide  use wide format
  |     Output modifiers
  <cr>

Cisco#show users
    Line       User       Host(s)              Idle       Location
*   0 con 0    manager    idle                 00:00:00
    1 vty 0    manager    idle                 00:08:29 10.0.100.84
    2 vty 1    manager    idle                 00:00:44 10.0.100.87

  Interface    User               Mode         Idle     Peer Address

Cisco#show users wide ?
  |  Output modifiers
  <cr>

Cisco#show users wide
    Line       User       Host(s)              Idle       Location
*   0 con 0    manager    idle                 00:00:00
    1 vty 0    manager    idle                 00:00:09 10.0.100.84
    2 vty 1    manager    idle                 00:05:37 10.0.100.87
    3 vty 2                                    00:00:00
    4 vty 3                                    00:00:00
    5 vty 4                                    00:00:00
    6 vty 5                                    00:00:00
    7 vty 6                                    00:00:00
    8 vty 7                                    00:00:00
    9 vty 8                                    00:00:00
   10 vty 9                                    00:00:00
   11 vty 10                                   00:00:00
   12 vty 11                                   00:00:00
   13 vty 12                                   00:00:00
   14 vty 13                                   00:00:00
   15 vty 14                                   00:00:00
   16 vty 15                                   00:00:00

  Interface    User               Mode         Idle     Peer Address
```

i) Remote Management Sessions—Terminating

ArubaOS-Switch	Comware5	Cisco
ArubaOS-Switch# kill 3	<Comware5>free user-interface 25	Cisco# clear line 3
	<Comware5>free user-interface vty 0	Cisco# clear line vty 2
	Comware7	
	<Comware7>free user-interface 129	
	<Comware7>free line 129	

ArubaOS-Switch

```
ArubaOS-Switch# kill ?
 <1-7>                 Kill other active console, Telnet, or SSH sessions.
 <cr>

ArubaOS-Switch# kill 3

ArubaOS-Switch# show telnet

 Telnet Activity

 Source IP Selection: Outgoing Interface

 -------------------------------------------------------
 Session  : **  1
 Privilege: Manager
 From     : Console
 To       :
 -------------------------------------------------------
 Session  :     2
 Privilege: Manager
 From     : 10.0.100.87
 To       :
```

Comware5

```
<Comware5>free ?
  ftp             Free FTP user
  user-interface  User terminal interface
  web-users       Web management users

<Comware5>free user-interface ?
  INTEGER<0-40>  Specify one user terminal interface
  aux            Aux user terminal interface
  vty            Virtual user terminal interface

<Comware5>free user-interface 25 ?
  <cr>

<Comware5>free user-interface 25
Are you sure to free user-interface vty0? [Y/N]:y
 [OK]


<Comware5>free user-interface vty ?
  INTEGER<0-15>  Specify one user terminal interface

<Comware5>free user-interface vty 0
Are you sure to free user-interface vty0? [Y/N]:y
 [OK]




<Comware5>display users
The user application information of the user interface(s):
  Idx UI      Delay    Type Userlevel
F 0   AUX 0   00:00:00      3

 +    : Current operation user.
 F    : Current operation user work in async mode.
```

Comware7

```
<Comware7>free ?
  ftp             FTP configuration information
  line            Line
  user-interface  Line
  web             Web configuration

<Comware7>free user-interface ?
  INTEGER<0-192>  Specify one line
  aux             AUX line
  vty             Virtual type terminal (VTY) line


<Comware7>free user-interface 129 ?
  <cr>

<Comware7>free user-interface 129
Are you sure to free line vty0? [Y/N]:y
 [OK]


<Comware7>free line ?
  INTEGER<0-192>  Specify one line
  aux             AUX line
  vty             Virtual type terminal (VTY) line

<Comware7>free line 129 ?
  <cr>

<Comware7>free line 129
Are you sure to free line vty0? [Y/N]:y


<Comware7>display users
  Idx  Line    Idle       Time              Pid     Type
F 0    AUX 0   00:00:00   Mar 23 15:22:58   538
  130  VTY 1   00:05:31   Mar 23 15:45:49   621     TEL

Following are more details.
VTY 1   :
        Location: 10.1.1.108
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

Cisco

```
Cisco#clear line ?
  <0-16>   Line number
  console  Primary terminal line
  vty      Virtual terminal

Cisco#clear line 2
[confirm]
 [OK]

Cisco#clear line vty ?
  <0-15>  Line number

Cisco#clear line vty 1 ?
  <cr>

Cisco#clear line vty 1
[confirm]
 [OK]
```

```
Cisco#show users
    Line       User       Host(s)              Idle       Location
*   0 con 0    manager    idle                 00:00:00
    1 vty 0    manager    idle                 00:02:30 10.0.100.84

  Interface    User               Mode         Idle     Peer Address
```

j) Tech Support Information Output Listing

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch# show tech	<Comware>display diagnostic-information	Cisco#show tech-support

ArubaOS-Switch

```
ArubaOS-Switch# show tech ?
 all                    Display output of a predefined command sequence used by technical
                        support.
 buffers                Display output of a predefined command sequence used by technical
                        support.
 custom                 Display output of a predefined command sequence used by technical
                        support.
 igmp                   Display output of a predefined command sequence used by technical
                        support.
 instrumentation        Display output of a predefined command sequence used by technical
                        support.
 mesh                   Display output of a predefined command sequence used by technical
                        support.
 mstp                   Display output of a predefined command sequence used by technical
                        support.
 oobm                   Display output of a predefined command sequence used by technical
                        support.
 rapid-pvst             Display output of a predefined command sequence used by technical
                        support.
 route                  Display output of a predefined command sequence used by technical
                        support.
 smart-link             Display output of a predefined command sequence used by technical
                        support.
 statistics             Display output of a predefined command sequence used by technical
                        support.
 transceivers           Display output of a predefined command sequence used by technical
                        support.
 tunnel                 Display output of a predefined command sequence used by technical
                        support.
 vrrp                   Display output of a predefined command sequence used by technical
                        support.
 <cr>
```

Comware5

```
<Comware5>display diagnostic-information ?
  |     Matching output
  <cr>

<Comware5>display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:
```

Comware7

```
<Comware7>display diagnostic-information ?
  STRING          [drive][path][file name]
  flash:          Device name
  hardware        Hardware information for diagnosis
  infrastructure  Infrastructure information for diagnosis
  l2              L2 information for diagnosis
  l3              L3 information for diagnosis
  service         Service information for diagnosis
  slot1#flash:    Device name
  slot1#usba0:    Device name
  usba0:          Device name
  <cr>



<Comware7>display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:
```

Cisco

```
Cisco#show tech-support ?
  cef          CEF related information
  ipc          IPC related information
  ipmulticast  IP multicast related information
  ospf         OSPF related information
  page         Page through output
  password     Include passwords
  rsvp         IP RSVP related information
  |            Output modifiers
  <cr>
```

k) Filtering Output show running-config and display current-configuration

ArubaOS-Switch	Comware	Cisco
Note: entering `show running-config | ?` does not reveal this command operation		
	`<Comware>display current-configuration | ?`	`Cisco#show running-config | ?`
`ArubaOS-Switch# show running-config | include <text-to-find>`	`<Comware>display current-configuration | include <text-to-find>`	`Cisco#show running-config | include <text-to-find>`

ArubaOS-Switch

Note: entering `show running-config | ?` does not reveal this command operation

```
ArubaOS-Switch# show running-config | include <text-to-find>
```

Comware5

```
<Comware5>display current-configuration | ?
  begin    Begin with the line that matches
  exclude  Match the character strings excluding the regular expression
  include  Match the character strings including with the regular expression

<Comware5>display current-configuration | include ?
  TEXT  Regular expression
```

```
<Comware5>display current-configuration | include <text-to-find>
```

Comware7

```
<Comware7>display current-configuration | ?
  begin       Display the first line that matches the specified regular
              expression and all lines that follow
  by-linenum  Display configuration with line number
  exclude     Display all lines that do not match the specified regular
              expression
  include     Display all lines that match the specified regular expression

<Comware7>display current-configuration | include ?
  STRING<1-256>  Regular expression

<Comware7>display current-configuration | include <text-to-find>
```

Cisco

```
Cisco#show running-config | ?
  append    Append redirected output to URL (URLs supporting append operation
            only)
  begin     Begin with the line that matches
  count     Count number of lines which match regexp
  exclude   Exclude lines that match
  format    Format the output using the specified spec file
  include   Include lines that match
  redirect  Redirect output to URL
  section   Filter a section of output
  tee       Copy output to URL

Cisco#show running-config | include ?
  LINE  Regular Expression

Cisco#show running-config | include <text-to-find>
```

l) Motd

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# banner motd # Enter TEXT message. End with the character'#'	[Comware]header motd # Please input banner content, and quit with the character '#'.	Cisco(config)#banner motd # Enter TEXT message. End with the character '#'.

ArubaOS-Switch

```
ArubaOS-Switch(config)# banner motd #
Enter TEXT message.  End with the character'#'


 This is a secure lab network, do not connect to any production systems.

     Authorized users only!
#
```

Comware

```
[Comware]header motd #
Please input banner content, and quit with the character '#'.


This is a secure lab network, do not connect to any production systems.
```

```
    Authorized users only!
#
```

Cisco

```
Cisco(config)#banner motd #
Enter TEXT message.  End with the character '#'.


This is a secure lab network, do not connect to any production systems.

    Authorized users only!
#
```

m) Source Interface for Management Communications

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# ip source-interface ?		Cisco(config)#ip <service> source-interface ?
		Cisco(config)#<service> source-interface ?
ArubaOS-Switch(config)# ip source-interface all 10.0.111.21		
ArubaOS-Switch(config)# ip source-interface syslog vlan 1	[Comware]info-center loghost source Vlan-interface 1	Cisco(config)#logging source-interface vlan 1
ArubaOS-Switch(config)# ip source-interface radius 10.0.111.21	[Comware]radius nas-ip 10.0.111.31	Cisco(config)#ip radius source-interface vlan 1
ArubaOS-Switch(config)# ip source-interface tacacs 10.0.111.21	[Comware]hwtacacs nas-ip 10.0.111.31	Cisco(config)#ip tacacs source-interface vlan 1
	[Comware]ftp client source interface Vlan-interface 1	Cisco(config)#ip ftp source-interface vlan 1
ArubaOS-Switch(config)# ip source-interface tftp vlan 1	[Comware]tftp client source interface Vlan-interface 1	Cisco(config)#ip tftp source-interface vlan 1
ArubaOS-Switch(config)# ip source-interface sntp vlan 1	[Comware]ntp source-interface Vlan-interface 100	Cisco(config)#ntp source vlan 1
ArubaOS-Switch(config)# ip source-interface telnet vlan 1	[Comware]telnet client source interface Vlan-interface 1	Cisco(config)#ip telnet source-interface vlan 1
	[Comware]ssh client source interface Vlan-interface 1	Cisco(config)#ip ssh source-interface vlan 1
ArubaOS-Switch(config)# ip source-interface sflow 10.0.111.21	[Comware] sflow source ip 10.0.111.31	
ArubaOS-Switch(config)# snmp-server trap-source 10.0.111.21	[Comware]snmp-agent trap source Vlan-interface 1	Cisco(config)#snmp-server source-interface traps vlan 1
ArubaOS-Switch# show ip source-interface		

ArubaOS-Switch

```
ArubaOS-Switch(config)# ip source-interface ?
 radius                 The RADIUS protocol.
 sntp                   The SNTP protocol.
 syslog                 The syslog protocol.
 tacacs                 The TACACS+ protocol.
 telnet                 The Telnet protocol.
 tftp                   The TFTP protocol.
 sflow                  The sFlow protocol.
 all                    All protocols above.

ArubaOS-Switch(config)# ip source-interface all ?                   [note, same options for
 all]
 IP-ADDR                Specify an IP address.                  [protocols as seen in above]
 loopback               Specify a loopback interface.
 vlan                   Specify a VLAN interface.


ArubaOS-Switch(config)# ip source-interface all 10.0.111.21

ArubaOS-Switch(config)# ip source-interface telnet vlan 1


ArubaOS-Switch(config)# snmp-server trap-source ?
 IP-ADDR                IP Address for the source ip address field in the trap
                        pdu.
 loopback               For the specified loopback interface, lexicographically
                        minimum configured ip address will be used as the source
                        ip address in the trap pdu.

ArubaOS-Switch(config)# snmp-server trap-source 10.0.111.21


ArubaOS-Switch# show ip source-interface ?
 detail                 Show detailed source IP information.
 radius                 Specify the protocol.
 sflow                  Specify the protocol.
 sntp                   Specify the protocol.
 status                 Show source IP information.
 syslog                 Specify the protocol.
 tacacs                 Specify the protocol.
 telnet                 Specify the protocol.
 tftp                   Specify the protocol.
 <cr>

ArubaOS-Switch# show ip source-interface

 Source-IP Configuration Information

  Protocol | Admin Selection Policy  IP Interface   IP Address
  -------- + ----------------------- -------------- ---------------
  Tacacs   | Configured IP Address   vlan-1         10.0.111.21
  Radius   | Configured IP Address   vlan-1         10.0.111.21
  Syslog   | Configured IP Interface vlan-1
  Telnet   | Configured IP Interface vlan-1
  Tftp     | Configured IP Interface vlan-1
  Sntp     | Configured IP Interface vlan-1
  Sflow    | Configured IP Address   vlan-1         10.0.111.21
```

Comware5

```
[Comware5]info-center loghost ?
  STRING<1-255>  Logging host ip address or hostname
  ipv6           Specify an IPv6 address
  source         Set the source address of packets sent to loghost
```

```
  vpn-instance   Specify a VPN instance

[Comware5]info-center loghost source ?
  Vlan-interface  VLAN interface

[Comware5]info-center loghost source Vlan-interface 1 ?
  <cr>

[Comware5]info-center loghost source Vlan-interface 1


[Comware5]radius nas-ip 10.0.111.31

[Comware5]hwtacacs nas-ip 10.0.111.31

[Comware5]ftp client source interface Vlan-interface 1

[Comware5]tftp client source interface Vlan-interface 1

[Comware5]ntp source-interface Vlan-interface 1

[Comware5]telnet client source interface Vlan-interface 1

[Comware5]ssh client source interface Vlan-interface 1

[Comware5]sflow source ip 10.0.111.31

[Comware5]snmp-agent trap source Vlan-interface 1
```

Comware7

```
[Comware7]ntp source Vlan-interface 1
```

Cisco

```
Cisco(config)#logging source-interface ?
  Async               Async interface
  Auto-Template       Auto-Template interface
  BVI                 Bridge-Group Virtual Interface
  CTunnel             CTunnel interface
  Dialer              Dialer interface
  FastEthernet        FastEthernet IEEE 802.3
  Filter              Filter interface
  Filtergroup         Filter Group interface
  GigabitEthernet     GigabitEthernet IEEE 802.3z
  GroupVI             Group Virtual interface
  Lex                 Lex interface
  Loopback            Loopback interface
  Null                Null interface
  Port-channel        Ethernet Channel of interfaces
  Portgroup           Portgroup interface
  Pos-channel         POS Channel of interfaces
  TenGigabitEthernet  Ten Gigabit Ethernet
  Tunnel              Tunnel interface
  Vif                 PGM Multicast Host interface
  Virtual-Template    Virtual Template interface
  Virtual-TokenRing   Virtual TokenRing
  Vlan                Catalyst Vlans
  fcpa                Fiber Channel

Cisco(config)#logging source-interface vlan 1 ?
  <cr>

Cisco(config)#logging source-interface vlan 1
```

```
(the following service commands are similar the above logging example)

Cisco(config)#ip radius source-interface vlan 1

Cisco(config)#ip tacacs source-interface vlan 1

Cisco(config)#ip ftp source-interface vlan 1

Cisco(config)#ip tftp source-interface vlan 1

Cisco(config)#ntp source vlan 1

Cisco(config)#ip telnet source-interface vlan 1

Cisco(config)#ip ssh source-interface vlan 1

Cisco(config)#snmp-server source-interface traps vlan 1
```

Chapter 2 Switch User ID and Password, and Console Access

This chapter focuses on:

- Configuring local user ID (uid) and password (pw) options
- Recovering from a lost password
- Protecting the local password
- Role based management
- Password complexity

For network access, Comware requires uid/pw and Cisco requires at least pw, while ArubaOS-Switch does not require either.

Network access methods for device management are covered in Chapters 8 and 9. Configuration details for Telnet and SSH are found in Chapter 8, and HTTP and HTTPS are found in Chapter 9.

a) Local User ID and Password, and console access

ArubaOS-Switch	Comware5	Cisco
		Cisco(config)#enable password 0 <password>
		Cisco(config)#enable secret 0 <password>
	[Comware5]super password level 3 simple password	
	[Comware5]super password level 3 cipher password	
ArubaOS-Switch(config)# password manager user-name <name> plaintext <password>	[Comware5]local-user <name> [Comware5-luser-manager]password simple <password> [Comware5-luser-manager]authorization-attribute level 3 [Comware5-luser-manager]service-type terminal	Cisco(config)#username <name> privilege 15 password <password>
ArubaOS-Switch(config)# password operator user-name <name> plaintext <password>	[Comware5]local-user <name> [Comware5-luser-operator]password simple <password> [Comware5-luser-operator]authorization-attribute level 1 [Comware5-luser-manager]service-type terminal	Cisco(config)#username <name> privilege 0 password <password>

	[Comware5]local-user <name> [Comware5-luser-manager]password cipher <password> [Comware5-luser-manager]authorization-attribute level 3 [Comware5-luser-manager]service-type terminal	
	[Comware5]local-user <name> [Comware5-luser-operator]password cipher <password> [Comware5-luser-operator]authorization-attribute level 1 [Comware5-luser-manager]service-type terminal	
	[Comware5]user-interface aux 0 [Comware5-ui-aux0]authentication-mode scheme	Cisco(config)#line console 0 Cisco(config-line)#login local
	[Comware5]user-interface aux 0 [Comware5-ui-aux0]authentication-mode password [Comware5-ui-aux0]set authentication password simple password	Cisco(config)#line console 0 Cisco(config-line)#login Cisco(config-line)#password password
ArubaOS-Switch (config)# password configuration-control		Cisco(config)#password <password>
ArubaOS-Switch (config)# password configuration history		Cisco(config)#aaa common-criteria policy policy1
ArubaOS-Switch (config)# password configuration aging		Cisco(config)#username username common-criteria-policy policy-name password <password>

ArubaOS-Switch (config)# password configuration alert-before-expiry 10		Cisco(config)#config switchconfig strong-pwd {case-check | consecutive-check | default-check | username-check | all-checks} {enable| disable}
ArubaOS-Switch (config)# password configuration update-interval-time 0		
ArubaOS-Switch (config)# password configuration expired-user-login 30		Cisco(config)#service paasword-encryption
	Comware7	
	[Comware7]super password role network-admin simple password	
	[Comware7]super password role network-admin hash <hashtext password>	
	[Comware7]local-user manager [Comware7-luser-manage-manager]password simple password [Comware7-luser-manage-manager]authorization-attribute user-role network-admin [Comware7-luser-manage-manager]service-type terminal	
	[Comware7]local-user <name> [Comware7-luser-manage-operator]password simple <password> [Comware7-luser-manage-operator]authorization-attribute user-role network-operator [Comware7-luser-manage-operator]service-type terminal	

	[Comware7]local-user manager [Comware7-luser-manage-manager]password hash <hashtext password> [Comware7-luser-manage-manager]authorization-attribute user-role network-admin [Comware7-luser-manage-manager]service-type terminal	
	[Comware7]local-user <name> [Comware7-luser-manage-operator]password hash <hashtext password> [Comware7-luser-manage-operator]authorization-attribute user-role network-operator [Comware7-luser-manage-operator]service-type terminal	
	[Comware7]user-interface aux 0 [Comware7-line-aux0]authentication-mode scheme	
	[Comware7]user-interface aux 0 [Comware7-line-aux0]authentication-mode password [Comware7-line-aux0]set authentication password simple password	

ArubaOS-Switch

```
ArubaOS-Switch(config)# password ?
 operator              Configure operator access.
 manager               Configure manager access.
 all                   Configure all available types of access.
 minimum-length        Configure minimum password length.

ArubaOS-Switch(config)# password manager ?
 plaintext             Enter plaintext password.
 user-name             Set username for the specified user category.
 <cr>

ArubaOS-Switch(config)# password manager user-name ?
 OCTET-STR             Enter an octet string.

ArubaOS-Switch(config)# password manager user-name manager ?
 plaintext             Enter plaintext password.
 <cr>

ArubaOS-Switch(config)# password manager user-name manager plaintext ?
PASSWORD              Specify the password.If in enhanced secure-mode, you will be
                      prompted for the password.

ArubaOS-Switch(config)# password manager user-name manager plaintext password ?
 <cr>

ArubaOS-Switch(config)# password manager user-name manager plaintext password

ArubaOS-Switch(config)# password operator user-name operator plaintext password
```

Note: If 'user-name' is not configured for either the manager or operator category, then "manager" and "operator" are the default user names respectively.

Comware5

```
[Comware5]super ?
  authentication-mode  Super authentication mode
  password             Specify the password

[Comware5]super password ?
  cipher  Specify password with cipher text
  hash    Save and display the hash value of the password
  level   Specify the entering password of the specified priority
  simple  Specify password with plain text

[Comware5]super password level ?
  INTEGER<1-3>  Priority level

[Comware5]super password level 3 ?
  cipher  Specify password with cipher text
  hash    Save and display the hash value of the password
  simple  Specify password with plain text

[Comware5]super password level 3 simple ?
  STRING<1-16>  Plain text password string

[Comware5]super password level 3 simple password ?
  <cr>

[Comware5]super password level 3 simple password

[Comware5]super password level 3 cipher password ?
  <cr>
```

```
[Comware5]super password level 3 cipher password

[Comware5]super password level 3 hash simple ?
  STRING<1-16>  Plain text password string

[Comware5]super password level 3 hash simple password ?
  <cr>


[Comware5]local-user ?
  STRING<1-55>           Specify the user name, the max length of username is 55
                         characters and the domainname can not be included.

[Comware5]local-user manager ?
  <cr>

[Comware5]local-user manager
New local user added.

[Comware5-luser-manager]?
Luser view commands:
  access-limit             Specify access limit of local user
  authorization-attribute  Specify authorization attribute of user
  bind-attribute           Specify bind attribute of user
  cfd                      Connectivity fault detection (IEEE 802.1ag)
  display                  Display current system information
  expiration-date          Specify expiration date configuration information
  group                    Specify user group of user
  mtracert                 Trace route to multicast source
  password                 Specify password of local user
  password-control         Specify password control
  ping                     Ping function
  quit                     Exit from current command view
  return                   Exit to User View
  save                     Save current configuration
  service-type             Specify service-type of local user
  state                    Specify state of local user
  tracert                  Trace route function
  undo                     Cancel current setting
  validity-date            Specify validity date configuration information

[Comware5-luser-manager]password ?
  cipher  Specify a ciphertext password
  hash    Save and display the hash value of the password
  simple  Specify a plaintext password
  <cr>

[Comware5-luser-manager]password simple ?
  STRING<1-63>  Plaintext password string

[Comware5-luser-manager]password simple password ?
  <cr>

[Comware5-luser-manager]password simple password

[Comware5-luser-manager]authorization-attribute ?
  acl              Specify ACL number of user
  callback-number  Specify dialing character string for callback user
  idle-cut         Specify idle-cut of local user
  level            Specify level of user
  user-profile     Specify user profile of user
  user-role        Specify role of local user
```

```
  vlan             Specify VLAN ID of user
  work-directory   Specify directory of user

[Comware5-luser-manager]authorization-attribute level ?
  INTEGER<0-3>  Level of user

[Comware5-luser-manager]authorization-attribute level 3 ?
  acl              Specify ACL number of user
  callback-number  Specify dialing character string for callback user
  idle-cut         Specify idle-cut of local user
  user-profile     Specify user profile of user
  user-role        Specify role of local user
  vlan             Specify VLAN ID of user
  work-directory   Specify directory of user
  <cr>

[Comware5-luser-manager]authorization-attribute level 3

[Comware5-luser-manager]service-type ?
  ftp         FTP service type
  lan-access  LAN-ACCESS service type
  portal      Portal service type
  ssh         Secure Shell service type
  telnet      TELNET service type
  terminal    TERMINAL service type
  web         Web service type

[Comware5-luser-manager]service-type terminal ?
  ssh     Secure Shell service type
  telnet  TELNET service type
  <cr>

[Comware5-luser-manager]service-type terminal


[Comware5-luser-manager]password ?
  cipher  Display password with cipher text
  simple  Display password with plain text

[Comware5-luser-manager]password cipher ?
  STRING<1-117>  Ciphertext password string

[Comware5-luser-manager]password cipher password
```

[the next command sets the use of uid/pw for login via console, even though the scheme is defined for AAA, it works with local uid/pw configuration]

```
[Comware5]user-interface aux 0

[Comware5-ui-aux0]?
User-interface view commands:
  acl                  Specify acl filtering
  activation-key       Specify a character to begin a terminal session
  authentication-mode  Terminal interface authentication mode
  auto-execute         Do something automatically
  cfd                  Connectivity fault detection (IEEE 802.1ag)
  command              Specify command configuration information
  databits             Specify the databits of user terminal interface
  display              Display current system information
  escape-key           Specify a character to abort a process started by
                       previously executed command
```

```
  flow-control          Specify the flow control mode of user terminal interface
  history-command       Record history command
  idle-timeout          Specify the connection idle timeout for login user
  mtracert              Trace route to multicast source
  parity                Specify the parity mode of user interface
  ping                  Ping function
  protocol              Set user interface protocol
  quit                  Exit from current command view
  return                Exit to User View
  save                  Save current configuration
  screen-length         Specify the lines displayed on one screen
  set                   Specify user terminal interface parameters
  shell                 Enable terminal user service
  speed                 Specify the TX/RX rate of user terminal interface
  stopbits              Specify the stop bit of user terminal interface
  terminal              Specify terminal type
  tracert               Trace route function
  undo                  Cancel current setting
  user                  Specify user's parameter of terminal interface

[Comware5-ui-aux0]authentication-mode ?
  none      Login without checking
  password  Authentication use password of user terminal interface
  scheme    Authentication use AAA

[Comware5-ui-aux0]authentication-mode scheme ?
  <cr>

[Comware5-ui-aux0]authentication-mode scheme
```

[the next command sets the use of password only for login via console]

```
[Comware5]user-interface aux 0

[Comware5-ui-aux0]authentication-mode password ?
  <cr>

[Comware5-ui-aux0]authentication-mode password

[Comware5-ui-aux0]set authentication password ?
  cipher  Set the password with cipher text
  hash    Save and display the hash value of the password
  simple  Set the password with plain text

[Comware5-ui-aux0]set authentication password simple ?
  STRING<1-16>  Plain text password

[Comware5-ui-aux0]set authentication password simple password ?
  <cr>

[Comware5-ui-aux0]set authentication password simple password
```

Comware7

```
[Comware7]super ?
  authentication-mode  Specify the authentication mode for user role switching
  default              Default target user role
  password             Set the password used to switch to a user role

[Comware7]super password ?
  hash    Specify a hashtext password
  role    Specify the user role
  simple  Specify a plaintext password
```

```
  <cr>

[Comware7]super password role ?
  STRING<1-63>      User role name
  network-admin
  network-operator
  level-0
  level-1
  level-2
  level-3
  level-4
  level-5
  level-6
  level-7
  level-8
  level-9
  level-10
  level-11
  level-12
  level-13
  level-14
  level-15
  security-audit

[Comware7]super password role network-admin ?
  hash    Specify a hashtext password
  simple  Specify a plaintext password
  <cr>

[Comware7]super password role network-admin simple ?
  STRING<1-63>  Plaintext password string

[Comware7]super password role network-admin simple password ?
  <cr>

[Comware7]super password role network-admin simple password

[Comware7]super password role network-admin hash ?
  STRING<1-110>  Hashtext password string

[Comware7]super password role network-admin hash password ?
  <cr>

[Comware7]super password role network-admin hash password


[Comware7]local-user ?
   STRING<1-55>  Local user name, which cannot contain the domain name

[Comware7]local-user manager ?
  <cr>

[Comware7]local-user manager
New local user added.

[Comware7-luser-manage-manager]?
Local-user protocol view commands:
  access-limit             Specify the maximum concurrent access number for the
                           local user
  authorization-attribute  Specify authorization attributes of local user
  bind-attribute           Specify binding attributes of local user
  cfd                      Connectivity Fault Detection (CFD) module
  diagnostic-logfile       Diagnostic log file configuration
```

```
  display                   Display current system information
  group                     Specify user group of local user
  logfile                   Log file configuration
  monitor                   System monitor
  password                  Specify password of local user
  password-control          Password control feature
  ping                      Ping function
  quit                      Exit from current command view
  return                    Exit to User View
  save                      Save current configuration
  security-logfile          Security log file configuration
  service-type              Specify a service type for the local user
  state                     Specify state of local user
  tracert                   Tracert function
  undo                      Cancel current setting

[Comware7-luser-manage-manager]password ?
  hash    Specify a hashtext password
  simple  Specify a plaintext password
  <cr>

[Comware7-luser-manage-manager]password simple ?
  STRING<1-63>  Plaintext password string

[Comware7-luser-manage-manager]password simple password ?
  <cr>

[Comware7-luser-manage-manager]password simple password

[Comware7-luser-manage-manager]authorization-attribute ?
  acl               Specify ACL of local user
  callback-number   Specify PPP callback number of local user
  idle-cut          Specify idle cut function for local user
  user-profile      Specify user profile of local user
  user-role         Specify user role of the local user
  vlan              Specify VLAN ID of local user
  work-directory    Specify work directory of local user

[Comware7-luser-manage-manager]authorization-attribute user-role ?
  STRING<1-63>      User role name
  network-admin
  network-operator
  level-0
  level-1
  level-2
  level-3
  level-4
  level-5
  level-6
  level-7
  level-8
  level-9
  level-10
  level-11
  level-12
  level-13
  level-14
  level-15
  security-audit

[Comware7-luser-manage-manager]authorization-attribute user-role network-admin ?

  acl               Specify ACL of local user
```

```
  callback-number  Specify PPP callback number of local user
  idle-cut         Specify idle cut function for local user
  user-profile     Specify user profile of local user
  vlan             Specify VLAN ID of local user
  work-directory   Specify work directory of local user
  <cr>

[Comware7-luser-manage-manager]authorization-attribute user-role network-admin

[Comware7-luser-manage-manager]service-type ?
  ftp       FTP service
  http      HTTP service type
  https     HTTPS service type
  pad       X.25 PAD service
  ssh       Secure Shell service
  telnet    Telnet service
  terminal  Terminal access service

[Comware7-luser-manage-manager]service-type terminal ?
  http    HTTP service type
  https   HTTPS service type
  pad     X.25 PAD service
  ssh     Secure Shell service
  telnet  Telnet service
  <cr>

[Comware7-luser-manage-manager]service-type terminal


[Comware7-luser-manage-manager]password ?
  hash    Specify a hashtext password
  simple  Specify a plaintext password
  <cr>

[Comware7-luser-manage-manager]password hash ?
  STRING<1-110>  Hashtext password string

[Comware7-luser-manage-manager]password hash password ?
  <cr>

[Comware7-luser-manage-manager]password hash password
```

[the next command sets the use of uid/pw for login via console, even though the scheme is defined for AAA, it works with local uid/pw configuration]

```
[Comware7]user-interface aux 0

[Comware7-line-aux0]?
Line view commands:
  activation-key       Specify a character to begin a terminal session
  authentication-mode  Login authentication mode
  auto-execute         Automatic execution configuration
  cfd                  Connectivity Fault Detection (CFD) module
  command              Command authorization and accounting
  databits             Set the databits of line
  diagnostic-logfile   Diagnostic log file configuration
  display              Display current system information
  escape-key           Escape key sequence configuration
  flow-control         Set a flow control mode
  history-command      History command buffer configuration
  idle-timeout         User connection idle timeout
```

```
  logfile               Log file configuration
  monitor               System monitor
  parity                Set the parity check method
  ping                  Ping function
  protocol              Set the protocols to be supported by the line
  quit                  Exit from current command view
  return                Exit to User View
  save                  Save current configuration
  screen-length         Specify the number of lines to be displayed on a screen
  security-logfile      Security log file configuration
  set                   Specify line parameters
  shell                 Enable terminal user service
  speed                 Line transmission speed
  stopbits              Specify the stop bit of line
  terminal              Specify terminal attribute
  tracert               Tracert function
  undo                  Cancel current setting
  user-role             Specify user role configuration information


[Comware7-line-aux0]authentication-mode ?
  none      Login without authentication
  password  Password authentication
  scheme    Authentication use AAA

[Comware7-line-aux0]authentication-mode scheme ?
  <cr>

[Comware7-line-aux0]authentication-mode scheme
```

[the next command sets the use of password only for login via console]

```
[Comware7]user-interface aux 0

[Comware7-line-aux0]authentication-mode password ?
  <cr>

[Comware7-line-aux0]authentication-mode password

[Comware7-line-aux0]set ?
  authentication  Specify the authentication parameters for line

[Comware7-line-aux0]set authentication ?
  password  Specify the password of line

[Comware7-line-aux0]set authentication password ?
  hash    Specify a hashtext password
  simple  Specify a plaintext password

[Comware7-line-aux0]set authentication password simple ?
  STRING<1-16>  Plaintext password string

[Comware7-line-aux0]set authentication password simple password  ?
  <cr>

[Comware7-line-aux0]set authentication password simple password
```

Cisco

```
Cisco(config)#enable ?
  last-resort  Define enable action if no TACACS servers respond
  password     Assign the privileged level password (MAX of 25 characters)
  secret       Assign the privileged level secret (MAX of 25 characters)
```

```
  use-tacacs   Use TACACS to check enable passwords

Cisco(config)#enable password ?
  0      Specifies an UNENCRYPTED password will follow
  7      Specifies a HIDDEN password will follow
  LINE   The UNENCRYPTED (cleartext) 'enable' password
  level  Set exec level password

Cisco(config)#enable password 0 ?
  LINE  The UNENCRYPTED (cleartext) 'enable' password

Cisco(config)#enable password 0 password ?
LINE    <cr>

Cisco(config)#enable password 0 password

Cisco(config)#enable secret ?
  0      Specifies an UNENCRYPTED password will follow
  5      Specifies an ENCRYPTED secret will follow
  LINE   The UNENCRYPTED (cleartext) 'enable' secret
  level  Set exec level password

Cisco(config)#enable secret 0 ?
  LINE  The UNENCRYPTED (cleartext) 'enable' secret

Cisco(config)#enable secret 0 secret ?
LINE    <cr>

Cisco(config)#enable secret 0 secret

Cisco(config)#username ?
  WORD  User name

Cisco(config)#username manager ?
  aaa                 AAA directive
  access-class        Restrict access by access-class
  autocommand         Automatically issue a command after the user logs in
  callback-dialstring Callback dialstring
  callback-line       Associate a specific line with this callback
  callback-rotary     Associate a rotary group with this callback
  dnis                Do not require password when obtained via DNIS
  mac                 This entry is for MAC Filtering where username=mac
  nocallback-verify   Do not require authentication after callback
  noescape            Prevent the user from using an escape character
  nohangup            Do not disconnect after an automatic command
  nopassword          No password is required for the user to log in
  password            Specify the password for the user
  privilege           Set user privilege level
  secret              Specify the secret for the user
  user-maxlinks       Limit the user's number of inbound links
  view                Set view name
  <cr>

Cisco(config)#username manager privilege ?
  <0-15>  User privilege level

Cisco(config)#username manager privilege 15 ?
  aaa                 AAA directive
  access-class        Restrict access by access-class
  autocommand         Automatically issue a command after the user logs in
  callback-dialstring Callback dialstring
  callback-line       Associate a specific line with this callback
  callback-rotary     Associate a rotary group with this callback
```

```
  dnis                  Do not require password when obtained via DNIS
  mac                   This entry is for MAC Filtering where username=mac
  nocallback-verify     Do not require authentication after callback
  noescape              Prevent the user from using an escape character
  nohangup              Do not disconnect after an automatic command
  nopassword            No password is required for the user to log in
  password              Specify the password for the user
  privilege             Set user privilege level
  secret                Specify the secret for the user
  user-maxlinks         Limit the user's number of inbound links
  view                  Set view name
  <cr>

Cisco(config)#username manager privilege 15 password ?
  0     Specifies an UNENCRYPTED password will follow
  7     Specifies a HIDDEN password will follow
  LINE  The UNENCRYPTED (cleartext) user password

Cisco(config)#username manager privilege 15 password password ?
LINE    <cr>

Cisco(config)#username manager privilege 15 password password

Cisco(config)#username operator privilege 0 password password
```

[the next command sets the use of uid/pw for login via console]

```
Cisco(config)#line console 0

Cisco(config-line)#login ?
  local   Local password checking
  <cr>

Cisco(config-line)#login local ?
  <cr>
Cisco(config-line)#login local
```

[the next command sets the use of password for login via console]

```
Cisco(config)#line console 0

Cisco(config-line)#login
% Login disabled on line 0, until 'password' is set

Cisco(config-line)#password ?
  0     Specifies an UNENCRYPTED password will follow
  7     Specifies a HIDDEN password will follow
  LINE  The UNENCRYPTED (cleartext) line password

Cisco(config-line)#password 0 password ?
LINE    <cr>

Cisco(config-line)#password 0 password
```

b) Recover Lost Password

ArubaOS-Switch	Comware	Cisco
See details below	See details below	See details below

Each procedure requires direct access to the switch through a console cable.

ArubaOS-Switch

Requires direct access to the switch (option 3 requires console cable). Default front panel security settings has all three options enabled.

Option 1) erase local usernames/passwords by depressing front panel clear button for one second. Requires physical access to switch.

Option 2) execute a factory reset by using a combination/sequence of the "clear" button and the "reset" button (reference product documentation for details). Requires physical access to switch.

Option 3) password recovery procedure requires direct access to the switch (with console cable) and calling HPE Networking technical support (reference product documentation for details).

Comware

Requires direct access to the switch (with console cable).

If password recovery capability is enabled (which is the default setting), a console user can access the device configuration without authentication and reconfigure the console login password and user privilege level passwords.

If password recovery capability is disabled, a console user must restore the factory-default configuration before configuring new passwords. Restoring the factory-default configuration deletes the next-startup configuration files.

Availability of related BootROM options varies with different versions of Comware.

```
Press Ctrl-B to enter Boot Menu... 1
BootRom password: Not required. Please press Enter to continue.

Password recovery capability is disabled.

   BOOT  MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Reserved
9. Set switch startup mode
0. Reboot
Ctrl+F: Format File System
```

```
Ctrl+D: Enter Debugging Mode
Ctrl+T: Enter Board Test Environment

Enter your choice(0-9):
```

Select 7 in order for switch to load its default configuration file, then select 0 to Reboot the switch.

Cisco

Depending on configuration of the "password-recovery" feature (see section c, Protect Local Password), there are two methods available; both require direct access to the switch (with console cable) and depressing the appropriate front panel button.

See the Cisco product documentation for exact procedure.

c) Protect Local Password

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# no front-panel-security password-clear	<Comware>undo startup bootrom-access enable	Cisco(config)#no service password-recovery
ArubaOS-Switch(config)# no front-panel-security factory-reset		
ArubaOS-Switch(config)# no front-panel-security password-recovery		
ArubaOS-Switch# show front-panel-security	<Comware>display startup	Cisco#show version

ArubaOS-Switch

Show state of front panel security:

```
ArubaOS-Switch# show front-panel-security

Clear Password        - Enabled
  Reset-on-clear      - Disabled
Factory Reset         - Enabled
Password Recovery     - Enabled


ArubaOS-Switch(config)# front-panel-security
 factory-reset         Enable/Disable factory-reset ability
 password-clear        Enable/Disable password clear
 password-recovery     Enable/Disable password recovery.


ArubaOS-Switch(config)# no front-panel-security password-clear
                              **** CAUTION ****
Disabling the clear button prevents switch passwords from being easily reset or recovered.
Ensure that you are familiar with the front panel security options before proceeding.
Continue with disabling the clear button [y/n]? y


ArubaOS-Switch(config)# no front-panel-security factory-reset
                              **** CAUTION ****
Disabling the factory reset option prevents switch configuration and passwords from being
easily reset or recovered.  Ensure that you are familiar with the front panel security
options before proceeding.
Continue with disabling the factory reset option[y/n]? y


ArubaOS-Switch(config)# no front-panel-security password-recovery
```

(Physical access procedure required.)

```
ArubaOS-Switch(config)# front-panel-security password-recovery help
Usage: [no] front-panel-security password-recovery
```

```
Description: Enable/Disable password recovery. To disable 'password-recovery'
             physical access to the front-panel is required.  Within 60 seconds
             of pressing the clear button, execute the 'no' form of the command.


ArubaOS-Switch# show front-panel-security
Clear Password        - Disabled
Factory Reset         - Disabled
Password Recovery     - Enabled
```

Note – ArubaOS-Switch ASIC will only allow up to two (2) of the above features to be disabled at a time, with one of them being the "clear" button disable, and then choice of the second feature to disable if desired.

Comware

As noted in section b, if password recovery capability is disabled, a console user must restore the factory-default configuration before configuring new passwords. Restoring the factory-default configuration deletes the next-startup configuration files.

In addition Comware5 supports an additional feature to disable access to the Boot ROM during the initial boot process.

From the HP 5500 EI & 5500 SI Switch Series Configuration Guide:

"By default, anyone can press Ctrl+B during startup to enter the Boot menu and configure the Boot ROM.

To protect the system, you can disable Boot ROM access so the users can access only the CLI.

You can also set a Boot ROM password the first time you access the Boot menu to protect the Boot ROM."

From the HP 5500 EI & 5500 SI Switch Series Command References guide:

Use *`undo startup bootrom-access enable`* to disable Boot ROM access during system startup (that is, you cannot enter the Boot ROM menu no matter whether you press Ctrl+B or not).

```
<Comware5>display startup
MainBoard:
 Current startup saved-configuration file: flash:/Comware_main.cfg
 Next main startup saved-configuration file: flash:/Comware_main.cfg
 Next backup startup saved-configuration file: NULL
 Bootrom-access enable state: enabled


<Comware>undo startup bootrom-access enable


<Comware5>display startup
MainBoard:
 Current startup saved-configuration file: flash:/Comware_main.cfg
 Next main startup saved-configuration file: flash:/Comware_main.cfg
```

```
 Next backup startup saved-configuration file: NULL
 Bootrom-access enable state: disabled
```

Cisco

From the Cisco Catalyst 3750 Switch Software Configuration Guide:

"By default, any end user with physical access to the switch can recover from a lost password by interrupting the boot process while the switch is powering on and then by entering a new password.

The password-recovery disable feature protects access to the switch password by disabling part of this functionality. When this feature is enabled, the end user can interrupt the boot process only by agreeing to set the system back to the default configuration. With password recovery disabled, you can still interrupt the boot process and change the password, but the configuration file (config.text) and the VLAN database file (vlan.dat) are deleted."

```
Cisco#show version
...
The password-recovery mechanism is enabled.
...


Cisco(config)#no service password-recovery


Cisco#show version
...
The password-recovery mechanism is disabled.
...
```

d) Role based management

ArubaOS-Switch	Comware7	Cisco
		Cisco(config)#aaa new-model
ArubaOS-Switch(config)# aaa authorization commands local	[Comware7]role name network-admin2	Cisco(config)#parser view network-admin2 Cisco(config-view)#secret 0 password
ArubaOS-Switch(config)# aaa authorization group network-admin2 1 match-command "command:show interface brief" permit log	[Comware7-role-network-admin2]rule 1 permit command display interface brief	Cisco(config-view)#commands exec include show interface summary
ArubaOS-Switch(config)# aaa authorization group network-admin2 2 match-command "command:show ip " permit log	[Comware7-role-network-admin2]rule 2 permit command display ip interface brief	Cisco(config-view)#commands exec include show ip interface brief
ArubaOS-Switch(config)# aaa authentication local-user test1 group network-admin2 password plaintext New password for test1: ******** Please retype new password for test1: ********	[Comware7]local-user test1 class manage [Comware7-luser-manage-test1]password simple password	Cisco(config-view)#exit Cisco(config)#username test1 privilege 15 view network-admin2 password 0 password
	[Comware7-luser-manage-test1]service-type telnet	
	[Comware7-luser-manage-test1]authorization-attribute user-role network-admin2	
	[Comware7-luser-manage-test1]undo authorization-attribute user-role network-operator	
ArubaOS-Switch# show authorization group network-admin2	[Comware7]display role name network-admin2 [Comware7]display local-user user-name test1 class manage	(no specific show commands)

ArubaOS-Switch

```
ArubaOS-Switch(config)# aaa authorization ?
 commands              Configure command authorization.
 group                 Create or remove an authorization rule.

ArubaOS-Switch(config)# aaa authorization commands ?
 access-level          Configure command authorization level.
 local                 Authorize commands using local groups.
 radius                Authorize commands using RADIUS.
 none                  Do not require authorization for command access.
 auto                  Authorize commands with the same protocol used for authentication.
 tacacs                Authorize commands using TACACS+.

ArubaOS-Switch(config)# aaa authorization commands local ?
 <cr>
ArubaOS-Switch(config)# aaa authorization commands local
```

```
ArubaOS-Switch(config)# aaa authorization group ?
 GROUPNAME-STR         The group name.

ArubaOS-Switch(config)# aaa authorization group network-admin2 ?
 <1-2147483647>        The sequence number.

ArubaOS-Switch(config)# aaa authorization group network-admin2 1 ?
 match-command         Specify the command to match.

ArubaOS-Switch(config)# aaa authorization group network-admin2 1 match-command ?
 COMMAND-STR           The command to match.

ArubaOS-Switch(config)# aaa authorization group network-admin2 1 match-command "command:show
interfaces brief" ?

 permit                Permit the specified action.
 deny                  Deny the specified action.

ArubaOS-Switch(config)# aaa authorization group network-admin2 1 match-command "command:show
interface brief" permit ?

 log                   Generate an event log any time a match happens.
 <cr>

ArubaOS-Switch(config)# aaa authorization group network-admin2 1 match-command "command:show
interface brief" permit log ?

 <cr>

ArubaOS-Switch(config)# aaa authorization group network-admin2 1 match-command "command:show
interface brief" permit log

ArubaOS-Switch(config)# aaa authorization group network-admin2 2 match-command "command:show
ip
" permit log

ArubaOS-Switch(config)# aaa authentication ?
 allow-vlan            Configure authenticator ports to apply VLAN changes immediately.
 captive-portal        Configure redirection to a captive portal server for additional
                       client authentication.
 console               Configure authentication mechanism used to control access to the
                       switch console.
 disable-username      Bypass the username during authentication while accessing the
                       switch to get Manager or Operator access.
 local-user            Create or remove a local user account.
 lockout-delay         The number of seconds after repeated login failures before a user
                       may again attempt login.
 login                 Specify that switch respects the authentication server's privilege
                       level.
 mac-based             Configure authentication mechanism used to control mac-based port
                       access to the switch.
 num-attempts          The number of login attempts allowed.
 port-access           Configure authentication mechanism used to control access to the
                       network.
 ssh                   Configure authentication mechanism used to control SSH access to
                       the switch.
 telnet                Configure authentication mechanism used to control Telnet access
                       to the switch.
 web                   Configure authentication mechanism used to control web access to
                       the switch.
 web-based             Configure authentication mechanism used to control web-based port
                       access to the switch.
```

```
ArubaOS-Switch(config)# aaa authentication local-user ?
 USERNAME-STR          The username.

ArubaOS-Switch(config)# aaa authentication local-user test1 ?
 aging-period          Configures the password aging time for a user.
 clear-history-record  Clears the history of the password for a user.
 group                 Specify the group for a username.
 min-pwd-length        Configures the minimum password length for a user.

ArubaOS-Switch(config)# aaa authentication local-user test1 group ?
 GROUPNAME-STR         The group name.

ArubaOS-Switch(config)# aaa authentication local-user test1 group network-admin2 ?
 password              Specify the password.
 <cr>

ArubaOS-Switch(config)# aaa authentication local-user test1 group network-admin2 password ?
 plaintext             Use plain text password.
 sha1                  Use SHA-1 hash.

ArubaOS-Switch(config)# aaa authentication local-user test1 group network-admin2 password
plaint
ext ?

 <cr>

ArubaOS-Switch(config)# aaa authentication local-user test1 group network-admin2 password
plaint
ext
New password for test1: ********
Please retype new password for test1: ********




ArubaOS-Switch# show authorization group ?
 GROUPNAME-STR         The group name.
 <cr>

ArubaOS-Switch# show authorization group network-admin2

 Local Management Groups - Authorization Information

  Group Name            : network-admin2
  Group Privilege Level : 4

  Users
  ----------------
  test1

  Seq. Num.  | Permission Rule Expression                          Log
  ---------- + ---------- ------------------------------------------ -------
  1          | Permit     command:show interfaces brief              Enable
  2          | Permit     command:show ip                            Enable
```

Comware5

Not an available feature

Comware7

```
[Comware7]role ?
  default-role   Specify the default user role configuration
  feature-group  Specify a feature group
  name           Specify a name for the user role

 [Comware7]role name ?
  STRING<1-63>  User role name

[Comware7]role name network-admin2 ?
  <cr>

[Comware7]role name network-admin2
[Comware7-role-network-admin2]%Jun 25 21:48:33:154 2016 Comware7 RBAC/6/INFO: Anonymous user
created role network-admin2 successfully.

[Comware7-role-network-admin2]?
Role view commands:
  cfd                 Connectivity Fault Detection (CFD) module
  description         Describe the user role
  diagnostic-logfile  Diagnostic log file configuration
  display             Display current system information
  interface           Specify the privilege of processing interface
  ip                  Specify IP configuration
  logfile             Log file configuration
  monitor             System monitor
  ping                Ping function
  quit                Exit from current command view
  return              Exit to User View
  rule                Specify a privilege control rule for the user role
  save                Save current configuration
  security-logfile    Security log file configuration
  tracert             Tracert function
  undo                Cancel current setting
  vlan                Specify the privilege of processing VLAN
  vpn-instance        Specify the privilege of processing VPN instance

[Comware7-role-network-admin2]rule ?
  INTEGER<1-256>  Rule number

[Comware7-role-network-admin2]rule 1 ?
  deny    Deny access to the matched commands
  permit  Permit access to the matched commands

[Comware7-role-network-admin2]rule 1 permit ?
  command  Specify a command matching string
  execute  Specify the execute (X) type commands
  read     Specify the read (R) type commands
  write    Specify the write (W) type commands

[Comware7-role-network-admin2]rule 1 permit command ?
  TEXT<1-128>  Command matching string. It may comprise multiple segments
               separated by semicolons. Each segment represents one or more
               commands and can contain multiple wildcards (*). The commands of
               the next segment, if any, must be subcommands of the previous
               segment.

[Comware7-role-network-admin2]rule 1 permit command display interface brief ?
  TEXT<1-104>  Command matching string. It may comprise multiple segments
               separated by semicolons. Each segment represents one or more
               commands and can contain multiple wildcards (*). The commands of
               the next segment, if any, must be subcommands of the previous
               segment.
```

```
  <cr>

[Comware7-role-network-admin2]rule 1 permit command display interface brief

[Comware7-role-network-admin2]rule 2 permit command display ip interface brief

Comware7]local-user ?
  STRING<1-55>  Local user name, which cannot contain the domain name

[Comware7]local-user test1 ?
  class  Specify a class for the local user
  <cr>

[Comware7]local-user test1 class ?
  manage   Device management user
  network  Network access user

[Comware7]local-user test1 class manage ?
  <cr>

[Comware7]local-user test1 class manage
New local user added.

[Comware7-luser-manage-test1]?
Local-user protocol view commands:
  access-limit             Specify the maximum concurrent access number for the
                           local user
  authorization-attribute  Specify authorization attributes of local user
  bind-attribute           Specify binding attributes of local user
  cfd                      Connectivity Fault Detection (CFD) module
  diagnostic-logfile       Diagnostic log file configuration
  display                  Display current system information
  group                    Specify user group of local user
  ip                       Specify IP configuration
  logfile                  Log file configuration
  monitor                  System monitor
  password                 Specify password of local user
  password-control         Password control feature
  ping                     Ping function
  quit                     Exit from current command view
  return                   Exit to User View
  save                     Save current configuration
  security-logfile         Security log file configuration
  service-type             Specify a service type for the local user
  state                    Specify state of local user
  tracert                  Tracert function
  undo                     Cancel current setting

[Comware7-luser-manage-test1]password ?
  hash    Specify a hashtext password
  simple  Specify a plaintext password
  <cr>

[Comware7-luser-manage-test1]password simple ?
  STRING<1-63>  Plaintext password string

[Comware7-luser-manage-test1]password simple password ?
  <cr>

[Comware7-luser-manage-test1]password simple password

[Comware7-luser-manage-test1]service-type ?
  ftp       FTP service
```

```
  http      HTTP service type
  https     HTTPS service type
  pad       X.25 PAD service
  ssh       Secure Shell service
  telnet    Telnet service
  terminal  Terminal access service

[Comware7-luser-manage-test1]service-type telnet ?
  http      HTTP service type
  https     HTTPS service type
  pad       X.25 PAD service
  ssh       Secure Shell service
  terminal  Terminal access service
  <cr>

[Comware7-luser-manage-test1]service-type telnet

[Comware7-luser-manage-test1]authorization-attribute ?
  acl              Specify ACL of local user
  callback-number  Specify PPP callback number of local user
  idle-cut         Specify idle cut function for local user
  user-profile     Specify user profile of local user
  user-role        Specify user role of the local user
  vlan             Specify VLAN ID of local user
  work-directory   Specify work directory of local user

[Comware7-luser-manage-test1]authorization-attribute user-role ?
  STRING<1-63>      User role name
  network-admin
  network-operator
  level-0
  level-1
  level-2
  level-3
  level-4
  level-5
  level-6
  level-7
  level-8
  level-9
  level-10
  level-11
  level-12
  level-13
  level-14
  level-15
  security-audit
  network-admin2

[Comware7-luser-manage-test1]authorization-attribute user-role network-admin2 ?
  acl              Specify ACL of local user
  callback-number  Specify PPP callback number of local user
  idle-cut         Specify idle cut function for local user
  user-profile     Specify user profile of local user
  vlan             Specify VLAN ID of local user
  work-directory   Specify work directory of local user
  <cr>

[Comware7-luser-manage-test1]authorization-attribute user-role network-admin2

[Comware7-luser-manage-test1]undo authorization-attribute user-role network-operator
```

```
[Comware7]display role ?
  >              Redirect it to a file
  >>             Redirect it to a file in append mode
  feature        Specify a feature
  feature-group  Specify a feature group
  name           Specify a name for the user role
  |              Matching output
  <cr>

[Comware7]display role name ?
  STRING<1-63>      User role name
  network-admin
  network-operator
  level-0
  level-1
  level-2
  level-3
  level-4
  level-5
  level-6
  level-7
  level-8
  level-9
  level-10
  level-11
  level-12
  level-13
  level-14
  level-15
  security-audit
  network-admin2

[Comware7]display role name network-admin2 ?
  >     Redirect it to a file
  >>    Redirect it to a file in append mode
  |     Matching output
  <cr>

[Comware7]display role name network-admin2
Role: network-admin2
  Description:
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------
  1       permit       command       display interface brief
  2       permit       command       display ip interface brief
  R:Read W:Write X:Execute

[Comware7]display local-user ?
  >             Redirect it to a file
  >>            Redirect it to a file in append mode
  class         Specify a class for the local user
  idle-cut      Display local users with idle cut function
  service-type  Display local users of specified service type
  state         Display local users in state of active or block
  user-name     Display local users using specified user name
  vlan          Display local users in specified VLAN
  |             Matching output
  <cr>
```

```
[Comware7]display local-user user-name ?
  STRING<1-55>  User name

[Comware7]display local-user user-name test1 ?
  class  Specify a class for the local user

[Comware7]display local-user user-name test1 class ?
  manage   Device management user
  network  Network access user

[Comware7]display local-user user-name test1 class manage ?
  >     Redirect it to a file
  >>    Redirect it to a file in append mode
  |     Matching output
  <cr>

[Comware7]display local-user user-name test1 class manage
Total 1 local users matched.

Device management user test1:
 State:                    Active
 Service type:             Telnet
 User group:               system
 Bind attributes:
 Authorization attributes:
  Work directory:          flash:
  User role list:          network-admin2
```

Cisco

```
Cisco(config)#aaa new-model

Cisco(config)#parser ?
  cache    Configure parser cache
  command  Configure command serialization
  config   Configure config generation
  maximum  specify performance maximums for CLI operations
  view     View Commands

Cisco(config)#parser view ?
  WORD  View Name

Cisco(config)#parser view network-admin2 ?
  superview  SuperView Commands
  <cr>

Cisco(config)#parser view network-admin2

Cisco(config-view)#?
View commands:
  commands  Configure commands for a view
  default   Set a command to its defaults
  exit      Exit from view configuration mode
  no        Negate a command or set its defaults
  secret    Set a secret for the current view

Cisco(config-view)#secret ?
  0     Specifies an UNENCRYPTED password will follow
  5     Specifies an ENCRYPTED secret will follow
  LINE  The UNENCRYPTED (cleartext) view secret string
```

```
Cisco(config-view)#secret 0 ?
  LINE  The UNENCRYPTED (cleartext) view secret string

Cisco(config-view)#secret 0 password ?
LINE    <cr>

Cisco(config-view)#secret 0 password

Cisco(config-view)#commands ?
  SASL-profile                    SASL profile configuration mode
  aaa-attr-list                   AAA attribute list config mode
  aaa-user                        AAA user definition
  acct_mlist                      AAA accounting methodlist definitions
  address-family                  Address Family configuration mode
  archive                         Archive the router configuration mode
  arp-nacl                        ARP named ACL configuration mode
  bgp address-family              Address Family configuration mode
  call-home                       call-home config mode
  call-home-profile               call-home profile config mode
  cc-policy                       policy-map config mode
  cfg-af-topo                     Configure non-base topology mode
  cns-connect-config              CNS Connect Info Mode
  cns-connect-intf-config         CNS Connect Intf Info Mode
  cns-tmpl-connect-config         CNS Template Connect Info Mode
  conf-attr-map                   LDAP attribute map config mode
  conf-ldap-server                LDAP server config mode
  conf-ldap-sg                    LDAP server group config mode
  conf-rad-filter                 RADIUS filter config mode
  conf-rad-server                 RADIUS server config mode
  conf-tac-server                 Tacacs Server Definition
  config-sensor-cdplist           Subscriber CDP attribute list
  config-sensor-dhcplist          Subscriber DHCP attribute list
  config-sensor-lldplist          Subscriber LLDP attribute list
  configure                       Global configuration mode
  crypto-identity                 Crypto identity config mode
  crypto-ipsec-profile            IPSec policy profile mode
  crypto-keyring                  Crypto Keyring command mode
  crypto-map                      Crypto map config mode
  crypto-map-fail-close           Crypto map fail close mode
  crypto-transform                Crypto transform config mode
  dhcp                            DHCP pool configuration mode
  dhcp-class                      DHCP class configuration mode
  dhcp-guard                      IPv6 dhcp guard configuration mode
  dhcp-pool-class                 Per DHCP pool class configuration mode
  dhcp-relay-info                 DHCP class relay agent info configuration mode
  dhcp-subnet-secondary           Per DHCP secondary subnet configuration mode
  dot1x                           CTS dot1x configuration mode
  dot1x-credential-mode           dot1x credential profile configuration mode
  eap-mprofile-mode               eap method profile configuration mode
  eap-profile-mode                eap profile configuration mode
  eigrp_af_classic_submode        Address Family configuration mode
  eigrp_af_intf_submode           Address Family interfaces configuration mode
  eigrp_af_submode                Address Family configuration mode
  eigrp_af_topo_submode           Address Family Topology configuration mode
  eigrp_sf_intf_submode           Service Family interfaces configuration mode
  eigrp_sf_submode                Service Family configuration mode
  eigrp_sf_topo_submode           Service Family Topology configuration mode
  exec                            Exec mode
  extcomm-list                    IP Extended community-list configuration mode
  fallback-profile-mode           fallback profile configuration mode
  fh_applet                       FH Applet Entry Configuration
  fh_applet_trigger               FH Applet Trigger Configuration
```

```
  filterserver                    AAA filter server definitions
  flow-cache                      Flow aggregation cache config mode
  flow-sampler-map                Flow sampler map config mode
  flowexp                         Flow Exporter configuration mode
  flowmon                         Flow Monitor configuration mode
  flowrec                         Flow Record configuration mode
  identity-policy-mode            identity policy configuration mode
  identity-profile-mode           identity profile configuration mode
  if-topo                         Configure interface topology parameters
  interface                       Interface configuration mode
  ip-sla                          IP SLAs entry configuration
  ip-sla-dhcp                     IP SLAs dhcp configuration
  ip-sla-dns                      IP SLAs dns configuration
  ip-sla-ftp                      IP SLAs ftp configuration
  ip-sla-http                     IP SLAs http configuration
  ip-sla-http-rr                  IP SLAs HTTP raw request Configuration
  ip-sla-icmpEcho                 IP SLAs icmpEcho configuration
  ip-sla-pathEcho                 IP SLAs pathEcho configuration
  ip-sla-pathJitter               IP SLAs pathJitter configuration
  ip-sla-tcp                      IP SLAs tcpConnect configuration
  ip-sla-udpEcho                  IP SLAs udpEcho configuration
  ip-sla-udpJitter                IP SLAs udpJitter configuration
  ip-sla-video                    IP SLAs video configuration
  ipczone                         IPC Zone config mode
  ipczone-assoc                   IPC Association config mode
  ipenacl                         IP named extended access-list configuration
                                  mode
  iprbacl                         IP role-based access-list configuration mode
  ipsnacl                         IP named simple access-list configuration mode
  ipv6-router                     IPv6 router configuration mode
  ipv6-snooping                   IPv6 snooping mode
  ipv6acl                         IPv6 access-list configuration mode
  ipv6dhcp                        IPv6 DHCP configuration mode
  ipv6dhcpvs                      IPv6 DHCP Vendor-specific configuration mode
  ipv6rbacl                       IPv6 role-based access-list configuration mode
  isakmp-profile                  Crypto ISAKMP profile command mode
  kron-occurrence                 Kron Occurrence SubMode
  kron-policy                     Kron Policy SubMode
  line                            Line configuration mode
  log_config                      Log configuration changes made via the CLI
  mac-enacl                       MAC named extended ACL configuration mode
  mac_address_config              MAC address group configuration mode
  macro_auto_trigger_cfg          Configuration mode for autosmartport user
                                  triggers
  manual                          CTS manual configuration mode
  map-class                       Map class configuration mode
  map-list                        Map list configuration mode
  mka-policy                      MKA Policy config mode
  mmon-fmon                       Flow Monitor configuration mode
  mmon-fmon-if-inline             Flow Monitor inline configuration mode under
                                  inline policy
  mmon-fmon-pmap-inline           Flow Monitor inline configuration mode under
                                  policy class
  mstp_cfg                        MSTP configuration mode
  mt-flowspec                     mt flow specifier
  mt-path                         mt path-config
  mt-prof-perf                    mt profile perf-monitor
  mt-prof-perf-params             mt profile perf-monitor parameters
  mt-prof-perf-rtp-params         mt profile perf-monitor rtp parameters
  mt-prof-sys                     mt profile system
  mt-prof-sys-params              mt profile system parameters
  mt-sesparam                     mt session-params
  multicast-flows-classmap        multicast-classmap config mode
```

```
  nd-inspection                   IPv6 NDP inspection configuration mode
  nd-raguard                      IPv6 RA guard configuration mode
  null-interface                  Null interface configuration mode
  parser_test                     Test mode for internal test purposes
  policy-list                     IP Policy List configuration mode
  preauth                         AAA Preauth definitions
  profile-map                     profile-map config mode
  radius-attrl                    Radius Attribute-List Definition
  radius-da-locsvr                Radius Application configuration
  radius-locsvr-client            Radius Client configuration
  radius-policy-device-locsvr     Radius Application configuration
  radius-proxy-locsvr             Radius Application configuration
  radius-sesm-locsvr              Radius Application configuration
  rib_rwatch_test                 RIB_RWATCH test configuration mode
  route-map                       Route map config mode
  router                          Router configuration mode
  router-af-topology              Topology configuration mode
  router_eigrp_classic            EIGRP Router configuration classic mode
  router_eigrp_named              EIGRP Router configuration named mode
  rsvp-local-if-policy            RSVP local policy interface configuration mode
  rsvp-local-policy               RSVP local policy configuration mode
  rsvp-local-subif-policy         RSVP local policy sub-interface configuration
                                  mode
  saf_ec_cfg                      Saf external-clients configuration mode
  saf_ec_client_cfg               Saf external-client configuration mode
  sampler                         Sampler configuration mode
  scope                           scope configuration mode
  scope address-family            Address Family configuration mode
  scope address-family topology   Topology configuration mode
  sep-init-config                 WSMA Initiator profile Mode
  sep-listen-config               WSMA Listener profile Mode
  sf_client_reg_mode              service-family exec test mode
  sg-radius                       Radius Server-group Definition
  sg-tacacs+                      Tacacs+ Server-group Definition
  sisf-sourceguard                IPv6 sourceguarde mode
  ssh-pubkey                      SSH public key identification mode
  ssh-pubkey-server               SSH public key entry mode
  ssh-pubkey-user                 SSH public key entry mode
  subscriber-policy               Subscriber policy configuration mode
  tcl                             Tcl mode
  template                        Template configuration mode
  template-peer-policy            peer-policy configuration mode
  template-peer-session           peer-session configuration mode
  top-af-base                     AF base topology configuration mode
  top-talkers                     Netflow top talkers config mode
  tracking-config                 Tracking configuration mode
  transceiver                     Transceiver type config mode
  vc-class                        VC class configuration mode
  view                            View configuration mode
  vrf                             Configure VRF parameters
  vrf-af                          Configure IP VRF parameters
  wsma-config-agent               WSMA Config Agent Profile configuration mode
  wsma-exec-agent                 WSMA Exec Agent Profile configuration mode
  wsma-filesys-agent              WSMA FileSys Agent Profile configuration mode
  wsma-notify-agent               WSMA Notify Agent Profile configuration mode
  xml-app                         XML Application configuration mode
  xml-transport                   XML Transport configuration mode

Cisco(config-view)#commands exec ?
  exclude            Exclude the command from the view
  include            Add command to the view
  include-exclusive  Include in this view but exclude from others
```

```
Cisco(config-view)#commands exec include ?
  LINE  Keywords of the command
  all   wild card support

Cisco(config-view)#commands exec include show interface summary ?
LINE    <cr>

Cisco(config-view)#commands exec include show interface summary

Cisco(config-view)#commands exec include show ip interface brief

Cisco(config-view)#exit

Cisco(config)#username test1 privilege 15 view network-admin2 password 0 password
```

e) Password complexity

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# password minimum-length 10	[Comware]password-control enable	Cisco(config)#aaa new-model
ArubaOS-Switch(config)# password configuration-control	[Comware]password-control length 10	Cisco(config)#aaa common-criteria policy pwcomplex
ArubaOS-Switch(config)# password configuration aging	[Comware]password-control length enable	Cisco(config-cc-policy)#min-length 10
ArubaOS-Switch(config)# password configuration history	[Comware]password-control composition type-number 4 type-length 2	Cisco(config-cc-policy)#max-length 10
ArubaOS-Switch(config)# password complexity all	[Comware]password-control composition enable	Cisco(config-cc-policy)#numeric-count 2
	[Comware]password-control complexity same-character check	Cisco(config-cc-policy)#special-case 2
	[Comware]password-control complexity user-name check	Cisco(config-cc-policy)#upper-case 2
		Cisco(config-cc-policy)#lower-case 2
		Cisco(config-cc-policy)#exit
		Cisco(config)# #username manager privilege 15 common-criteria-policy pwcomplex password PA55word!^
ArubaOS-Switch# show password-configuration	[Comware]display password-control	Cisco#show aaa common-criteria policy name pwcomplex

ArubaOS-Switch

```
ArubaOS-Switch(config)# password ?
 operator              Configure operator access.
 manager               Configure manager access.
 all                   Configure all available types of access.
 clear-history-record  Clears the history of stored user passwords.
 complexity            Configures the password complexity function.
 composition           Configures the password composition policy for all users.
 configuration         Enables the password configuration aging, logon details and
                       history checks.
 configuration-control Enable the password configuration and complexity feature aligned
                       to UCR-2008 standard.
 minimum-length        Configure the minimum password length.

ArubaOS-Switch(config)# password minimum-length ?
 <0-64>

ArubaOS-Switch(config)# password minimum-length 10

ArubaOS-Switch(config)# password configuration-control ?
 <cr>

ArubaOS-Switch(config)# password configuration-control
The password configuration feature cannot be enabled when the WebUI is enabled.
Would you like to disable WebUI and REST protocol? [y/n]: y
```

```
ArubaOS-Switch(config)# password configuration ?
 aging                 Enables the password configuration aging check.
 aging-period          Configures the password aging time for a system.
 alert-before-expiry   Sets the number of days before password aging during which the
                       user is warned of the pending password expiration.
 expired-user-login    Configures additional logins within a specified period during
                       which a user is allowed to access the switch without changing an
                       expired password.
 history               Enables the password history check.
 history-record        Configures the maximum number of history password records for each
                       user.
 log-on-details        Disables execution of the 'show authentication last-login' command
                       so that the logon details are not displayed.
 update-interval-time  The period of waiting, in hours, before an existing password can
                       be changed.

ArubaOS-Switch(config)# password configuration aging ?
 aging
 aging-period

ArubaOS-Switch(config)# password configuration aging ?
 <cr>

ArubaOS-Switch(config)# password configuration aging

ArubaOS-Switch(config)# password configuration history ?
 history
 history-record

ArubaOS-Switch(config)# password configuration history ?
 <cr>

ArubaOS-Switch(config)# password configuration history

ArubaOS-Switch(config)# password complexity ?
 all                   Configures the repeat password character check, repeat password
                       check and user name check.
 repeat-char-check     Configuration to ensure that password does not contain three of
                       the same characters used consecutively.
 repeat-password-check Configures the repeat password character check.
 user-name-check       Ensures that the password does not contain repeat or reverse of
                       the associated username.

ArubaOS-Switch(config)# password complexity all ?
 <cr>
ArubaOS-Switch(config)# password complexity all



[As seen from the login screen]

Username: manager

Password:<password>                                  [note, password was not displayed)
Please change the password to logon to the system.
Old password:
New password:<PA55word!^zaQW@>                       [note, password was not displayed)
Re-enter the new password:



ArubaOS-Switch# show password-configuration
```

```
 Global password control configuration

  Password control                      : Enabled
  Password history                      : Enabled
  Number of history records             : 8
  Password aging                        : Enabled
  Aging time                            : 90 days
  Early notice on password expiration   : 7 days
  Minimum password update interval      : 24 hours
  Expired user login                    : 3 login attempts in 30 days
  Password minimum length               : 10
  User login details checking           : Enabled
  Password composition
           Lower case                   : 2 characters
           Upper case                   : 2 characters
           Special character            : 2 characters
           Number                       : 2 characters
  Repeat password checking              : Enabled
  Username checking                     : Enabled
  Repeat characters checking            : Enabled
```

Comware5

```
[Comware5]password-control ?
  aging                    Specify password aging time
  alert-before-expire      Specify alert time before password expired
  authentication-timeout   Specify authentication timeout
  complexity               Specify password complexity
  composition              Specify composition of password
  enable                   Enable password control globally
  expired-user-login       Specify user login with expired password
  history                  Specify maximum history record
  length                   Specify minimum length of password
  login                    Specify local user's login
  login-attempt            Specify local user's login attempts
  password                 Specify password
  super                    Super user's password controls

[Comware5]password-control enable ?
  <cr>

[Comware5]password-control enable ..
 Info: Password control is enabled.

[Comware5]password-control length ?
  INTEGER<4-32>  Minimum length of password(in characters)
  enable         Enable the password control function

[Comware5]password-control length 10 ?
  <cr>
[Comware5]password-control length 10

[Comware5]password-control length enable ?
  <cr>

[Comware5]password-control length enable
 Info: Password minimum length is enabled for all users.
```

```
[Comware5]password-control composition ?
  enable       Enable the password control function
  type-number  Specify minimum number of
               characters(case-letters,numbers,symbols) type

[Comware5]password-control composition type-number ?
  INTEGER<1-4>  Minimum types of characters the password contains

[Comware5]password-control composition type-number 4 ?
  type-length  Specify minimum characters for each required type
  <cr>

[Comware5]password-control composition type-number 4 type-length ?
  INTEGER<1-63>  Minimum characters of each required type contains

[Comware5]password-control composition type-number 4 type-length 2 ?
  <cr>

[Comware5]password-control composition type-number 4 type-length 2

[Comware5]password-control composition enable ?
  <cr>

[Comware5]password-control composition enable
 Info: Password composition is enabled for all users.

[Comware5]password-control complexity ?
  same-character  Specify same-character
  user-name       Specify username

[Comware5]password-control complexity same-character ?
  check  Enable password complexity checking at login

[Comware5]password-control complexity same-character check ?
  <cr>

[Comware5]password-control complexity same-character check
 Info: Check of password include repeat same char is enabled for all users.

[Comware5]password-control complexity user-name ?
  check  Enable password complexity checking at login

[Comware5]password-control complexity user-name check ?
  <cr>

[Comware5]password-control complexity user-name check
 Info: Check of password include username is enabled for all users.



[As seen from a login screen]

Login authentication


Username:manager
Password:<password>                        [note, password was not displayed)
Info: First logged in. For security reasons you will need to change your password.
 Please enter your new password.
Password:<PA55word!^>                      [note, password displayed as asterisks)
Confirm :**********
Updating user(s) information, please wait......
```

```
[As seen at the console screen]

#Jun 25 15:03:43:626 2016 Comware5 SHELL/4/LOGIN:
 Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1:manager login from VTY
%Jun 25 15:03:43:768 2016 Comware5 LS/4/LS_PWD_CHGPWD_FOR_FIRSTLOGIN: User manager changed
the password because first login.
%Jun 25 15:03:43:921 2016 Comware5 SHELL/5/SHELL_LOGIN: manager logged in from 10.1.1.109.



[Comware5]display password-control ?
  blacklist  Display blacklist information
  super      Display super user's password-control information
  |          Matching output
  <cr>

[Comware5]display password-control
 Global password control configurations:
 Password control:                    Enabled
 Password aging:                      Enabled (90 days)
 Password length:                     Enabled (10 characters)
 Password composition:                Enabled (4 types,  2 characters per type)
 Password history:                    Enabled (max history records:4)
 Early notice on password expiration: 7 days
 User authentication timeout:         60 seconds
 Maximum failed login attempts:       3 times
 Login attempt-failed action:         Lock for 1 minutes
 Minimum password update time:        24 hours
 User account idle-time:              90 days
 Login with aged password:            3 times in 30 days
 Password complexity:                 Enabled (username checking)
                                      Enabled (repeated characters checking)
```

Comware7

```
[Comware7]password-control ?
  aging                Specify password aging
  alert-before-expire  Set the alert time before password expiration
  complexity           Check password complexity
  composition          Specify password composition
  enable               Enable password control globally
  expired-user-login   Allow a user to log in with an expired password within a
                       period
  history              Specify maximum number of history passowrds for each user
  length               Specify minimum password length
  login                Specify local user login
  login-attempt        Control local user login attempts
  super                Super user's password controls
  update-interval      Set the minimum password update interval

[Comware7]password-control enable ?
  <cr>

[Comware7]password-control enable

[Comware7]password-control length ?
  INTEGER<4-32>  Minimum password length,in characters
  enable         Enable the password control function

[Comware7]password-control length 10 ?
```

```
  <cr>

[Comware7]password-control length 10

[Comware7]password-control length enable ?
  <cr>

[Comware7]password-control length enable

[Comware7]password-control composition ?
  enable       Enable the password control function
  type-number  Specify the minimum number of password composition types
               (letters, numbers, symbols)

[Comware7]password-control composition type-number ?
  INTEGER<1-4>  Minimum number of types

[Comware7]password-control composition type-number 4 ?
  type-length  Specify the minimum number of characters for each type
  <cr>

[Comware7]password-control composition type-number 4 type-length ?
  INTEGER<1-63>  Minimum number of characters

[Comware7]password-control composition type-number 4 type-length 2 ?
  <cr>

[Comware7]password-control composition type-number 4 type-length 2

[Comware7]password-control composition enable ?
  <cr>

[Comware7]password-control composition enable

[Comware7]password-control complexity ?
  same-character  Deny 3 or more repeated characters in password
  user-name       Deny username or reversed username in password

[Comware7]password-control complexity same-character ?
  check  Enable password complexity checking

[Comware7]password-control complexity same-character check ?
  <cr>

[Comware7]password-control complexity same-character check

[Comware7]password-control complexity user-name ?
  check  Enable password complexity checking

[Comware7]password-control complexity user-name check ?
  <cr>

[Comware7]password-control complexity user-name check



[As seen from a login screen]

login: manager
Password: <password>                          [note, password was not displayed)
First login or password reset. For security reason, you need to change your password. Please
enter your password.
old password: *********
```

```
new password: <PA55word!^>                    [note, password displayed as asterisks)
confirm: *********
Updating user information. Please wait ... ...

[As seen at the console screen]


[Comware7]%Jun 25 14:32:04:223 2016 Comware7 PWDCTL/6/CHANGEPASSWORD:  manager changed the
password because first login.
%Jun 25 14:32:05:645 2016 Comware7 SHELL/5/SHELL_LOGIN: manager logged in from 10.1.1.109.



[Comware7]display password-control ?
  >          Redirect it to a file
  >>         Redirect it to a file in append mode
  blacklist  Display blacklist user information
  super      Display the password control information of the super passwords
  |          Matching output
  <cr>

[Comware7]display password-control
 Global password control configurations:
 Password control:                    Enabled
 Password aging:                      Enabled (90 days)
 Password length:                     Enabled (10 characters)
 Password composition:                Enabled (4 types, 2 characters per type)
 Password history:                    Enabled (max history records:4)
 Early notice on password expiration: 7 days
 Maximum login attempts:              3
 Action for exceeding login attempts: Lock user for 1 minutes
 Minimum interval between two updates:24 hours
 User account idle time:              90 days
 Logins with aged password:           3 times in 30 days
 Password complexity:                 Enabled (username checking)
                                      Enabled (repeated characters checking)
```

Cisco

```
Cisco(config)#aaa ?
  accounting       Accounting configurations parameters.
  attribute        AAA attribute definitions
  authentication   Authentication configurations parameters.
  authorization    Authorization configurations parameters.
  cache            AAA cache definitions
  common-criteria  AAA Common Criteria
  configuration    Authorization configuration parameters.
  dnis             Associate certain AAA parameters to a specific DNIS number
  group            AAA group definitions
  local            AAA Local method options
  max-sessions     Adjust initial hash size for estimated max sessions
  memory           AAA memory parameters
  nas              NAS specific configuration
  new-model        Enable NEW access control commands and functions.(Disables
                   OLD commands.)
  password         Configure password/secret related settings
  pod              POD processing
  policy           AAA policy parameters
  server           Local AAA server
```

```
  service-profile  Service-Profile parameters
  session-id       AAA Session ID
  traceback        Traceback recording
  user             AAA user definitions

Cisco(config)#aaa new-model ?
  <cr>

Cisco(config)#aaa new-model

Cisco(config)#aaa common-criteria ?
  policy  Policy definition

Cisco(config)#aaa common-criteria policy ?
  WORD  Policy name

Cisco(config)#aaa common-criteria policy pwcomplex ?
  <cr>

Cisco(config)#aaa common-criteria policy pwcomplex

Cisco(config-cc-policy)#?
CC Policy commands:
  char-changes   Number of change characters between old and new passwords
  copy           Copy from policy
  exit           Exit from common-criteria sub-mode
  lifetime       lifetime configuration
  lower-case     Number of lower-case characters
  max-length     Specify the maximum length of the password
  min-length     Specify the minimum length of the password
  no             Negate a command or set its defaults
  numeric-count  Number of numeric characters
  special-case   Number of special characters
  upper-case     Number of upper-case characters

Cisco(config-cc-policy)#min-length ?
  <1-127>  Min Length 1-127

Cisco(config-cc-policy)#min-length 10 ?
  <cr>

Cisco(config-cc-policy)#min-length 10

Cisco(config-cc-policy)#max-length ?
  <1-127>  Max Length 1-127

Cisco(config-cc-policy)#max-length 10 ?
  <cr>

Cisco(config-cc-policy)#max-length 10

Cisco(config-cc-policy)#numeric-count ?
  <0-127>  Number of digits from 0-127

Cisco(config-cc-policy)#numeric-count 2 ?
  <cr>

Cisco(config-cc-policy)#numeric-count 2

Cisco(config-cc-policy)#special-case ?
  <0-127>  Number of special characters from 0-127

Cisco(config-cc-policy)#special-case 2 ?
```

```
  <cr>
Cisco(config-cc-policy)#special-case 2

Cisco(config-cc-policy)#upper-case ?
  <0-127>  Number of upper-case characters from 0-127

Cisco(config-cc-policy)#upper-case 2 ?
  <cr>

Cisco(config-cc-policy)#upper-case 2

Cisco(config-cc-policy)#lower-case ?
  <0-127>  Number of lower-case characters from 0-127

Cisco(config-cc-policy)#lower-case 2 ?
  <cr>

Cisco(config-cc-policy)#lower-case 2

Cisco(config-cc-policy)#exit


Cisco(config)#username manager privilege 15 ?
  aaa                     AAA directive
  access-class            Restrict access by access-class
  algorithm-type          Algorithm to use for hashing the plaintext secret for
                          the user
  autocommand             Automatically issue a command after the user logs in
  callback-dialstring     Callback dialstring
  callback-line           Associate a specific line with this callback
  callback-rotary         Associate a rotary group with this callback
  common-criteria-policy  Enter the common-criteria policy name
  dnis                    Do not require password when obtained via DNIS
  mac                     This entry is for MAC Filtering where username=mac
  nocallback-verify       Do not require authentication after callback
  noescape                Prevent the user from using an escape character
  nohangup                Do not disconnect after an automatic command
  nopassword              No password is required for the user to log in
  password                Specify the password for the user
  privilege               Set user privilege level
  secret                  Specify the secret for the user
  user-maxlinks           Limit the user's number of inbound links
  view                    Set view name
  <cr>

Cisco(config)#username manager privilege 15 common-criteria-policy ?
  WORD  Name of policy

Cisco(config)#username manager privilege 15 common-criteria-policy pwcomplex ?
  aaa                     AAA directive
  access-class            Restrict access by access-class
  algorithm-type          Algorithm to use for hashing the plaintext secret for
                          the user
  autocommand             Automatically issue a command after the user logs in
  callback-dialstring     Callback dialstring
  callback-line           Associate a specific line with this callback
  callback-rotary         Associate a rotary group with this callback
  common-criteria-policy  Enter the common-criteria policy name
  dnis                    Do not require password when obtained via DNIS
  mac                     This entry is for MAC Filtering where username=mac
  nocallback-verify       Do not require authentication after callback
  noescape                Prevent the user from using an escape character
  nohangup                Do not disconnect after an automatic command
```

```
  nopassword              No password is required for the user to log in
  password                Specify the password for the user
  privilege               Set user privilege level
  secret                  Specify the secret for the user
  user-maxlinks           Limit the user's number of inbound links
  view                    Set view name
  <cr>

Cisco(config)#username manager privilege 15 common-criteria-policy pwcomplex password ?
  0     Specifies an UNENCRYPTED password will follow
  7     Specifies a HIDDEN password will follow
  LINE  The UNENCRYPTED (cleartext) user password

Cisco(config)#username manager privilege 15 common-criteria-policy pwcomplex password
PA55word!^ ?

Cisco(config)#username manager privilege 15 common-criteria-policy pwcomplex password
PA55word!^
LINE    <cr>

Cisco(config)#username manager privilege 15 common-criteria-policy pwcomplex password
PA55word!^



Cisco#show aaa common-criteria policy name pwcomplex
Policy name: pwcomplex
Minimum length: 10
Maximum length: 10
Upper Count: 2
Lower Count: 2
Numeric Count: 2
Special Count: 2
Number of character changes 4
Valid forever. User tied to this policy will not expire
```

Chapter 3 Image or Operating System File Management

This chapter compares the commands used to manage software image or operating system files on ArubaOS-Switch, Comware, and Cisco.

The ArubaOS-Switch operating system writes to or reads from specific areas of the file storage, depending on the commands you enter. Image files, configuration files, and local user ID and passwords are stored in separate/dedicated areas of flash. When you enter commands such as **copy** and **show**, the ArubaOS-Switch operating system writes to or reads from these dedicated areas of flash. (For more information, see the management and configuration guide for the HP ArubaOS-Switch you are managing.)

Comware and Cisco platforms use basic file system operations. There are no dedicated areas of flash for specific files or file types. You are allowed to create subdirectories, and to copy and move files just as you would on other "regular" file systems.

ArubaOS-Switchescan store a maximum of two operating system files. With Comware and Cisco switches, the number of operating system files is limited only by the amount of available flash memory on the switch file system.

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch# show flash	<Comware>dir	Cisco#show flash:
ArubaOS-Switch# show version	<Comware>display version	Cisco#show version
ArubaOS-Switch# copy tftp flash 10.0.100.111 K_15_16_0004.swi	<Comware>tftp 10.0.100.111 get A5500EI-CMW520-R2221P07.bin	Cisco#copy tftp:// 10.0.100.111/c3750-advipservicesk9-mz.122-46.SE.bin flash: Destination filename [c3750e-universalk9-mz.150-2.SE7.bin]?
ArubaOS-Switch# copy sftp flash 10.0.100.111 K_15_16_0004.swi Attempting username/password authentication... Enter manager@10.0.100.111's password: ********	<Comware> scp 10.0.100.111 get A5500EI-CMW520-R2221P07.bin Username: manager Trying 10.0.100.111 ... Press CTRL+K to abort Connected to 10.0.100.111 ... Enter password:	Cisco#copy scp://10.0.100.111/c3750e-universalk9-mz.150-2.SE7.bin flash Source username [manager]? Destination filename [c3750e-universalk9-mz.150-2.SE7.bin]?
ArubaOS-Switch# copy usb flash K_15_16_0004.swi	<Comware7>copy usba0:/5900_5920-CMW710-R2311P05.ipe flash:/5900_5920-CMW710-R2311P05.ipe [note: Comware5 does not support usb]	
ArubaOS-Switch# copy xmodem flash	<Comware>xmodem get flash:/	Cisco#copy xmodem: flash:

	[Note: Comware7 does not support xmodem]	
ArubaOS-Switch# copy flash flash secondary		
ArubaOS-Switch# copy flash tftp 10.0.100.111 K_15_16_0004.swi	<Comware>tftp 10.0.100.111 put a5500ei-cmw520-r2221p07.bin	Cisco#copy flash: tftp: Source filename []? c3750e-universalk9-mz.150-1.SE.bin Address or name of remote host []? 10.0.100.111 Destination filename [c3750e-universalk9-mz.150-1.SE.bin]?
ArubaOS-Switch# copy flash sftp 10.0.100.111 K_15_16_0004.swi Attempting username/password authentication... Enter manager@10.0.100.111's password: ********	<Comware>scp 10.0.100.111 put a5500ei-cmw520-r2221p07.bin Username: manager Trying 10.0.100.111 ... Press CTRL+K to abort Connected to 10.0.100.111 ... Enter password:	Cisco#copy flash: scp: Source filename [c3750e-universalk9-mz.150-1.SE.bin]? Address or name of remote host []? 10.0.100.111 Destination username [manager]? Destination filename [c3750e-universalk9-mz.150-1.SE.bin]?
ArubaOS-Switch# copy flash usb K_15_16_0004.swi	<Comware7>copy flash:/5900_5920-CMW710-R2311P05.ipe usba0:/ [note: Comware5 does not support usb]	
ArubaOS-Switch# copy flash xmodem		
ArubaOS-Switch# boot set-default flash primary	<Comware>boot-loader file flash:/a5500ei-cmw520-r2221p07.bin slot 1 main	Cisco(config)# boot system flash:c3750-advipservicesk9-mz.122-46.SE.bin
ArubaOS-Switch(config)# activate-firmware check		Cisco(config)# license install *stored-location-url*

ArubaOS-Switch

```
ArubaOS-Switch# show flash
Image              Size (bytes) Date     Version
----------------- ------------ -------- --------------
Primary Image     :    16334377 11/19/14 KA.15.16.0005
Secondary Image   :    15842118 09/11/14 KA.15.15.0008

Boot ROM Version : KA.15.09
Default Boot     : Primary

ArubaOS-Switch# show version
Image stamp:
 /ws/swbuildm/rel_orlando_qaoff/code/build/tam(swbuildm_rel_orlando_qaoff_rel_orlando)
                Nov 19 2014 15:08:22
                KA.15.16.0005
                333
Boot Image:     Primary
```

```
ArubaOS-Switch# copy ?
 command-output        Specify a CLI command to copy output of.
 config                Copy named configuration file.
 core-dump             Copy coredump file from flash.
 crash-data            Copy the switch crash data file.
 crash-log             Copy the switch log file.
 default-config        Copy custom default configuration.
 event-log             Copy event log file.
 fdr-log               Copy FDR logs from the switch to TFTP server, USB or xmodem
                       terminal.
 flash                 Copy the switch system image file.
 running-config        Copy running configuration file.
 sftp                  Copy data from a SFTP server.
 ssh-client-known-h... Copy the known hosts file.
 ssh-server-pub-key    Copy the switch's SSH server public key.
 startup-config        Copy in-flash configuration file.
 tftp                  Copy data from a TFTP server.
 usb                   Copy data from a USB flash drive.
 xmodem                Use xmodem on the terminal as the data source.

ArubaOS-Switch# copy tftp ?
 autorun-cert-file     Copy autorun trusted certificate to the switch.
 autorun-key-file      Copy autorun key file to the switch.
 command-file          Copy command script to switch and execute.
 config                Copy data to the specified switch configuration file.
 default-config        Copy source file to custom default configuration.
 flash                 Copy data to the switch system image file.
 local-certificate     Local Certificate to be copied.
 pub-key-file          Copy the public keys to the switch.
 show-tech             Copy custom show-tech script to switch.
 ssh-client-key        Copy an RSA or DSA private key to the switch for the SSH client to
                       use.
 ssh-client-known-h... Copy a file containing SSH known hosts to the switch.
 startup-config        Copy data to the switch configuration file.
 ta-certificate        Copy a Trust Anchor certificate to the device.


ArubaOS-Switch# copy tftp flash ?
 HOST-NAME-STR         Specify hostname of the TFTP server.
 IP-ADDR               Specify TFTP server IPv4 address.
 IPV6-ADDR             Specify TFTP server IPv6 address.



ArubaOS-Switch# copy tftp flash 10.0.100.111 ?
 FILENAME-STR          Specify filename for the TFTP transfer.

ArubaOS-Switch# copy tftp flash 10.0.100.11 K_15_16_0004.swi ?
 primary               Copy to primary flash.
 secondary             Copy to secondary flash.
 oobm                  Use the OOBM interface to reach TFTP server.
 <cr>

ArubaOS-Switch# copy tftp flash 10.0.100.111 K_15_16_0004.swi secondary ?
 oobm                  Use the OOBM interface to reach TFTP server.
 <cr>

ArubaOS-Switch# copy tftp flash 10.0.100.111 K_15_16_0004.swi secondary


ArubaOS-Switch# copy sftp ?
 autorun-cert-file     Copy autorun trusted certificate to the switch.
```

```
 autorun-key-file      Copy autorun key file to the switch.
 command-file          Copy command script to switch and execute.
 config                Copy data to the specified switch configuration file.
 default-config        Copy source file to custom default configuration.
 flash                 Copy data to the switch system image file.
 local-certificate     Local Certificate to be copied.
 pub-key-file          Copy the public keys to the switch.
 show-tech             Copy custom show-tech script to switch.
 ssh-client-key        Copy an RSA or DSA private key to the switch for the SSH client to
                       use.
 ssh-client-known-h... Copy a file containing SSH known hosts to the switch.
 startup-config        Copy data to the switch configuration file.
 ta-certificate        Copy a Trust Anchor certificate to the device.

ArubaOS-Switch# copy sftp flash ?
 HOST-NAME-STR         Specify hostname of the SFTP server.
 IP-ADDR               Specify SFTP server IPv4 address.
 IPV6-ADDR             Specify SFTP server IPv6 address.
 user                  Specify the username on the remote system
 USERNAME@IP-STR       Specify the username along with remote system information
                       (hostname, IPv4 or IPv6 address).

ArubaOS-Switch# copy sftp flash 10.0.100.111 ?
 FILENAME-STR          Specify filename for the SFTP transfer
 port                  TCP port of the SSH server on the remote system.

ArubaOS-Switch# copy sftp flash 10.0.100.111 K_15_16_0004.swi ?
 primary               Copy to primary flash.
 secondary             Copy to secondary flash.
 oobm                  Use the OOBM interface to reach SFTP server.
 <cr>

ArubaOS-Switch# copy sftp flash 10.0.100.111 K_15_16_0004.swi secondary ?
 oobm                  Use the OOBM interface to reach SFTP server.
 <cr>
ArubaOS-Switch# copy sftp flash 10.0.100.111 K_15_16_0004.swi secondary
Attempting username/password authentication...
Enter manager@10.0.100.111's password: ********
SFTP download in progress.


ArubaOS-Switch# copy usb ?
 autorun-cert-file     Copy autorun trusted certificate to the switch.
 autorun-key-file      Copy autorun key file to the switch.
 command-file          Copy command script to switch and execute.
 config                Copy data to the specified switch configuration file.
 default-config        Copy custom default configuration to the switch.
 flash                 Copy data to the switch system image file.
 pub-key-file          Copy the public keys to the switch.
 ssh-client-key        Copy an RSA or DSA private key to the switch for the SSH client to
                       use.
 ssh-client-known-h... Copy a file containing SSH known hosts to the switch.
 startup-config        Copy data to the switch configuration file.

ArubaOS-Switch# copy usb flash ?
 IMAGE-NAME-STR        Specify filename for the USB transfer.

ArubaOS-Switch# copy usb flash K_15_16_0004.swi ?
 primary               Copy to primary flash.
 secondary             Copy to secondary flash.
 <cr>

ArubaOS-Switch# copy usb flash K_15_16_0004.swi secondary ?
```

```
 <cr>

ArubaOS-Switch# copy usb flash K_15_16_0004.swi secondary


ArubaOS-Switch# copy xmodem ?
 command-file          Copy command script to switch and execute.
 config                Copy data to the specified switch configuration file.
 default-config        Copy source file to custom default configuration.
 flash                 Copy to primary/secondary flash.
 ssh-client-key        Copy an RSA or DSA private key to the switch for the SSH client to
                       use.
 ssh-client-known-h... Copy a file containing SSH known hosts to the switch.
 startup-config        Copy data to the switch configuration file.

ArubaOS-Switch# copy xmodem flash ?
 primary               Copy to primary flash.
 secondary             Copy to secondary flash.
 <cr>

ArubaOS-Switch# copy xmodem flash secondary ?
 <cr>

ArubaOS-Switch# copy xmodem flash secondary
The Secondary OS Image will be deleted, continue [y/n]?  y
Press 'Enter' and start XMODEM on your host...


ArubaOS-Switch# copy flash ?
 flash                 Copy to primary/secondary flash.
 sftp                  Copy data to an SFTP server
 tftp                  Copy data to a TFTP server.
 usb                   Copy data to a USB flash drive.
 xmodem                Use xmodem on the terminal as the data destination.

ArubaOS-Switch# copy flash flash ?
 primary               Copy to primary flash.
 secondary             Copy to secondary flash.

ArubaOS-Switch# copy flash flash secondary


ArubaOS-Switch# copy flash tftp ?
 oobm                  Use the OOBM interface to reach TFTP server.
 IP-ADDR               Specify TFTP server IPv4 address.
 IPV6-ADDR             Specify TFTP server IPv6 address.

ArubaOS-Switch# copy flash tftp 10.0.100.111 ?
 FILENAME-STR          Specify filename for the TFTP transfer.

ArubaOS-Switch# copy flash tftp 10.0.100.111 K_15_16_0004.swi ?
 primary               Copy image primary flash.
 secondary             Copy image secondary flash.
 oobm                  Use the OOBM interface to reach TFTP server.
 <cr>

ArubaOS-Switch# copy flash tftp 10.0.100.111 K_15_16_0004.swi secondary ?
 oobm                  Use the OOBM interface to reach TFTP server.
 <cr>

ArubaOS-Switch# copy flash tftp 10.0.100.111 K_15_16_0004.swi secondary
```

```
ArubaOS-Switch# copy flash sftp 10.0.100.111 K_15_16_0004.swi ?
 primary               Copy image primary flash.
 secondary             Copy image secondary flash.
 oobm                  Use the OOBM interface to reach SFTP server.
 <cr>

ArubaOS-Switch# copy flash sftp 10.0.100.111 K_15_16_0004.swi secondary ?
 oobm                  Use the OOBM interface to reach SFTP server.
 <cr>
ArubaOS-Switch# copy flash sftp 10.0.100.111 K_15_16_0004.swi secondary
Attempting username/password authentication...
Enter manager@10.0.100.111's password: ********
SFTP download in progress.


ArubaOS-Switch# copy flash usb ?
 FILENAME-STR          Specify filename for the TFTP transfer.

ArubaOS-Switch# copy flash usb K_15_16_0004.swi ?
 primary               Copy image primary flash.
 secondary             Copy image secondary flash.
 <cr>

ArubaOS-Switch# copy flash usb K_15_16_0004.swi


ArubaOS-Switch# copy flash xmodem ?
 primary               Copy image primary flash.
 secondary             Copy image secondary flash.
 <cr>

ArubaOS-Switch# copy flash xmodem secondary ?
 <cr>

ArubaOS-Switch# copy flash xmodem
Press 'Enter' and start XMODEM on your host...


ArubaOS-Switch# boot ?
 set-default           Specify the default flash boot image for the next boot.
 system                Allows user to specify boot image to use after reboot.
 <cr>

ArubaOS-Switch# boot set-default ?
 flash                 Specify the default flash boot image for the next boot.

ArubaOS-Switch# boot set-default flash ?
 primary               Primary flash image.
 secondary             Secondary flash image.

ArubaOS-Switch# boot set-default flash primary ?
 <cr>

ArubaOS-Switch# boot set-default flash primary


ArubaOS-Switch(config)# activate-firmware service

disable                Disables Activate firmware service.

enable                 Enables Activate firmware service.
```

```
ArubaOS-Switch(config)# activate-firmware update

primary                Upgrades primary image.

secondary             Upgrades secondary image.
```

Comware5

In this chapter, SCP (Secure Copy) is used for secure file transfers. SFTP (Secure File Trasnfer Protocol) is used in Chapter 4 for secure file transfers.

```
<Comware5>dir ?
  /all               List all files
  /all-filesystems   List files on all filesystems
  STRING             [drive][path][file name]
  flash:             Device name
  <cr>


<Comware5>dir
Directory of flash:/

   0     -rw-      3816  Mar 06 2015 00:31:44   startup.cfg
   1     -rw-      8322  Feb 19 2015 17:04:50   config.cwmp
   2     drw-         -  Apr 26 2000 12:00:21   seclog
   3     -rw-    483732  Jan 23 2015 12:38:11   a5500ei-btm-721.btm
   4     -rw-       151  Mar 06 2015 00:31:39   system.xml
   5     -rw-      4096  Nov 10 2012 02:44:37   comware5_dhcp.txt
   6     -rw-  14274135  Jan 23 2015 13:10:35   a5500ei-cmw520-r2221p07.bin
   7     -rw-      2422  Nov 21 2012 06:44:59   https-server.p12

31496 KB total (17051 KB free)

<Comware5>display version
HP Comware Platform Software
Comware Software, Version 5.20.99, Release 2221P07
Copyright (c) 2010-2014 Hewlett-Packard Development Company, L.P.
HP A5500-24G-PoE+ EI Switch with 2 Interface Slots uptime is 0 week, 0 day, 0 hour, 38
minutes

HP A5500-24G-PoE+ EI Switch with 2 Interface Slots with 1 Processor
256M    bytes SDRAM
32768K  bytes Flash Memory

Hardware Version is REV.C
CPLD Version is 002
Bootrom Version is 721
[SubSlot 0] 24GE+4SFP+POE Hardware Version is REV.C


<Comware5>tftp ?
  STRING<1-20>  IP address or hostname of a remote system
  ipv6          IPv6 TFTP client

<Comware5>tftp 10.0.100.111 ?
  get   Download file from remote TFTP server
  put   Upload local file to remote TFTP server
  sget  Download securely from remote TFTP server

<Comware5>tftp 10.0.100.111 get ?
  STRING<1-135>  Source filename

<Comware5>tftp 10.0.100.111 get A5500EI-CMW520-R2221P07.bin ?
```

```
  STRING<1-135>  Destination filename
  source         Specify a source
  vpn-instance   Specify a VPN instance
  <cr>

<Comware5>tftp 10.0.100.111 get A5500EI-CMW520-R2221P07.bin


<Comware5>scp ?
  STRING<1-20>  Address or host name of the remote system
  ipv6          IPv6 protocol

<Comware5>scp 10.0.100.111 ?
  INTEGER<0-65535>  Port number
  get               Download a file
  put               Upload a file

<Comware5>scp 10.0.100.111 get ?
  STRING<1-135>  Source file name

<Comware5>scp 10.0.100.111 get A5500EI-CMW520-R2221P07.bin ?
  STRING<1-135>       Destination file name
  identity-key        Specify the algorithm for publickey authentication
  prefer-ctos-cipher  Specify the preferred encryption algorithm from client to
                      server
  prefer-ctos-hmac    Specify the preferred HMAC algorithm from client to
                      server
  prefer-kex          Specify the preferred key exchange algorithm
  prefer-stoc-cipher  Specify the preferred encryption algorithm from server to
                      client
  prefer-stoc-hmac    Specify the preferred HMAC algorithm from server to
                      client
  username            Specify the user name
  <cr>

<Comware5>scp 10.0.100.111 get A5500EI-CMW520-R2221P07.bin
Username: manager
Trying 10.0.100.111 ...
Press CTRL+K to abort
Connected to 10.0.100.111 ...
Enter password:


<Comware5>xmodem ?
  get  Obtain remote data file

<Comware5>xmodem get ?
  STRING  [drive][path][file name]
  flash:  Device name

<Comware5>xmodem get flash:/ ?
  <cr>

<Comware5>xmodem get flash:/


<Comware5>tftp 10.0.100.111 put a5500ei-cmw520-r2221p07.bin ?
  STRING<1-135>  Destination filename
  source         Specify a source
  vpn-instance   Specify a VPN instance
  <cr>

<Comware5>tftp 10.0.100.111 put a5500ei-cmw520-r2221p07.bin
```

```
<Comware5>scp 10.0.100.111 put a5500ei-cmw520-r2221p07.bin ?
  STRING<1-135>       Destination file name
  identity-key        Specify the algorithm for publickey authentication
  prefer-ctos-cipher  Specify the preferred encryption algorithm from client to
                      server
  prefer-ctos-hmac    Specify the preferred HMAC algorithm from client to
                      server
  prefer-kex          Specify the preferred key exchange algorithm
  prefer-stoc-cipher  Specify the preferred encryption algorithm from server to
                      client
  prefer-stoc-hmac    Specify the preferred HMAC algorithm from server to
                      client
  username            Specify the user name
  <cr>

<Comware5>scp 10.0.100.111 put a5500ei-cmw520-r2221p07.bin
Username: manager
Trying 10.0.100.111 ...
Press CTRL+K to abort
Connected to 10.0.100.111 ...
Enter password:


<Comware5>boot-loader ?
  file    File path
  update  Update image file

<Comware5>boot-loader file ?
  STRING  [drive][path][file name]
  flash:  Device name

<Comware5>boot-loader file flash:/a5500ei-cmw520-r2221p07.bin ?
  slot  Specify the slot number

<Comware5>boot-loader file flash:/a5500ei-cmw520-r2221p07.bin slot ?
  INTEGER<1>  Slot number
  all         All current slot number

<Comware5>boot-loader file flash:/a5500ei-cmw520-r2221p07.bin slot 1 ?
  backup  Set backup attribute
  main    Set main attribute

<Comware5>boot-loader file flash:/a5500ei-cmw520-r2221p07.bin slot 1 main ?
  <cr>

<Comware5>boot-loader file flash:/a5500ei-cmw520-r2221p07.bin slot 1 main
```

Comware7

In this chapter, SCP (Secure Copy) is used for secure file transfers. SFTP (Secure File Trasnfer Protocol) is used in Chapter 4 for secure file transfers.

```
<Comware7>dir ?
  /all              Display all files and directories in the current directory
  /all-filesystems  Display the files and directories in the root directories of
                    all storage media
  >                 Redirect it to a file
  >>                Redirect it to a file in append mode
  STRING            [drive][path][file name]
  flash:            Device name
  slot1#flash:      Device name
```

```
  slot1#usba0:      Device name
  usba0:            Device name
  |                 Matching output
  <cr>


<Comware7>dir
Directory of flash:
   1 -rw-    10986496 Feb 04 2015 17:52:26   5900_5920-cmw710-boot-r2416.bin
   2 -rw-    66350080 Feb 04 2015 17:54:43   5900_5920-cmw710-system-r2416.bin
   3 drw-           - Dec 31 2010 18:00:23   diagfile
   4 -rw-        1580 Mar 23 2015 18:30:53   ifindex.dat
   5 -rw-        5778 Mar 23 2015 18:30:54   startup.cfg
   6 -rw-      175617 Mar 23 2015 18:30:55   startup.mdb
   7 -rw-           0 Oct 06 2014 12:02:16   lauth.dat
   8 drw-           - Dec 31 2010 18:00:24   license
   9 drw-           - Jan 01 2011 18:00:23   logfile
  10 drw-           - Sep 15 2014 10:45:45   pki
  11 drw-           - Dec 31 2010 18:00:23   seclog
  12 drw-           - Feb 04 2015 18:00:57   versionInfo

524288 KB total (436412 KB free)


<Comware7>display version
HP Comware Software, Version 7.1.045, Release 2416
Copyright (c) 2010-2014 Hewlett-Packard Development Company, L.P.
HP 5900AF-48G-4XG-2QSFP+ Switch uptime is 0 weeks, 1 day, 2 hours, 46 minutes
Last reboot reason : Cold reboot

Boot image: flash:/5900_5920-cmw710-boot-r2416.bin
Boot image version: 7.1.045, Release 2416
  Compiled Dec 09 2014 16:02:10
System image: flash:/5900_5920-cmw710-system-r2416.bin
System image version: 7.1.045, Release 2416
  Compiled Dec 09 2014 16:02:10


Slot 1:
Uptime is 0 weeks,1 day,2 hours,46 minutes
5900AF-48G-4XG-2QSFP+ Switch with 2 Processors
BOARD TYPE:         5900AF-48G-4XG-2QSFP+ Switch
DRAM:               2048M bytes
FLASH:              512M bytes
PCB 1 Version:      VER.A
Bootrom Version:    139
CPLD 1 Version:     001
CPLD 2 Version:     255
Release Version:    HP 5900AF-48G-4XG-2QSFP+ Switch-2416
Patch Version  :    None
Reboot Cause  :     ColdReboot
[SubSlot 0] 48GE+4SFP Plus+2QSFP Plus


Comware7>tftp ?
  STRING<1-253>  IP address or hostname of the TFTP Server
  ipv6           IPv6 TFTP Client

<Comware7>tftp 10.0.100.111 ?
  get   Download a file from the TFTP server
  put   Upload a local file to the TFTP server
  sget  Download a file from the TFTP server securely
```

```
<Comware7>tftp 10.0.100.111 get ?
  STRING<1-255>  Source filename

<Comware7>tftp 10.0.100.111 get 5900_5920-CMW710-R2311P05.ipe ?
  STRING<1-255>  Destination filename
  dscp           Set the Differentiated Services Codepoint (DSCP) value
  source         Specify the source address for outgoing TFTP packets
  vpn-instance   Specify a VPN instance
  <cr>

<Comware7>tftp 10.0.100.111 get 5900_5920-CMW710-R2311P05.ipe
Press CTRL+C to abort.


<Comware7>scp ?
  STRING<1-253>  IP address or hostname of remote system
  ipv6           IPv6 information

<Comware7>scp 10.0.100.111 ?
  INTEGER<1-65535>  Specify port number
  get               Get file from server
  put               Put file to server
  vpn-instance      Specify a VPN instance

<Comware7>scp 10.0.100.111 get ?
  STRING<1-255>  Source file name

<Comware7>scp 10.0.100.111 get 5900_5920-CMW710-R2311P05.ipe ?
  STRING<1-255>       Destination file name
  identity-key        Specify the algorithm for publickey authentication
  prefer-compress     Specify the preferred compression algorithm
  prefer-ctos-cipher  Specify the preferred encryption algorithm from client to
                      server
  prefer-ctos-hmac    Specify the preferred HMAC algorithm from client to server
  prefer-kex          Specify the preferred key exchange algorithm
  prefer-stoc-cipher  Specify the preferred encryption algorithm from server to
                      client
  prefer-stoc-hmac    Specify the preferred HMAC algorithm from server to client
  publickey           Specify the public key of server
  source              Specify a source
  <cr>

<Comware7>scp 10.0.100.111 get 5900_5920-CMW710-R2311P05.ipe
Username: manager
Press CTRL+C to abort.
Connecting to 10.0.100.111 port 22.
manager@10.0.100.111's password:



<Comware7>copy usb?
  usba0:/

<Comware7>copy usba0:/?
  "usba0:/System Volume Information/"
  usba0:/5900_5920-CMW710-R2311P05.ipe
  usba0:/5900_5920-CMW710-R2416.ipe
  usba0:/5900_5920-cmw710-boot-r2311p05.bin
  usba0:/5900_5920-cmw710-boot-r2416.bin
  usba0:/5900_5920-cmw710-system-r2311p05.bin
  usba0:/5900_5920-cmw710-system-r2416.bin

<Comware7>copy usba0:/5900_5920-CMW710-R2311P05.ipe ?
```

```
  STRING        [drive][path][file name]
  flash:        Device name
  ftp:          File on the FTP server
  slot1#flash:  Device name
  slot1#usba0:  Device name
  tftp:         File on the TFTP server
  usba0:        Device name

<Comware7>copy usba0:/5900_5920-CMW710-R2311P05.ipe flash:/?
  flash:/5900_5920-cmw710-boot-r2416.bin
  flash:/5900_5920-cmw710-system-r2416.bin
  flash:/diagfile/
  flash:/ifindex.dat
  flash:/startup.cfg
  flash:/startup.mdb
  flash:/lauth.dat
  flash:/license/
  flash:/logfile/
  flash:/pki/
  flash:/seclog/
  flash:/versionInfo/

<Comware7>copy usba0:/5900_5920-CMW710-R2311P05.ipe flash:/5900_5920-CMW710-R2311P05.ipe ?
  <cr>

<Comware7>copy usba0:/5900_5920-CMW710-R2311P05.ipe flash:/5900_5920-CMW710-R2311P05.ipe


<Comware7>tftp 10.0.100.111 put 5900_5920-CMW710-R2311P05.ipe ?
  STRING<1-255>  Destination filename
  dscp           Set the Differentiated Services Codepoint (DSCP) value
  source         Specify the source address for outgoing TFTP packets
  vpn-instance   Specify a VPN instance
  <cr>

<Comware7>tftp 10.0.100.111 put 5900_5920-CMW710-R2311P05.ipe


<Comware7>scp 10.0.100.111 put 5900_5920-CMW710-R2311P05.ipe ?
  STRING<1-255>       Destination file name
  identity-key        Specify the algorithm for publickey authentication
  prefer-compress     Specify the preferred compression algorithm
  prefer-ctos-cipher  Specify the preferred encryption algorithm from client to
                      server
  prefer-ctos-hmac    Specify the preferred HMAC algorithm from client to server
  prefer-kex          Specify the preferred key exchange algorithm
  prefer-stoc-cipher  Specify the preferred encryption algorithm from server to
                      client
  prefer-stoc-hmac    Specify the preferred HMAC algorithm from server to client
  publickey           Specify the public key of server
  source              Specify a source
  <cr>

<Comware7>scp 10.0.100.111 put 5900_5920-CMW710-R2311P05.ipe
Username: manager
Press CTRL+C to abort.
Connecting to 10.0.100.111 port 22.
manager@10.0.100.111's password:


<Comware7>copy flash:/?
  flash:/5900_5920-CMW710-R2311P05.ipe
  flash:/5900_5920-cmw710-boot-r2416.bin
```

```
  flash:/5900_5920-cmw710-system-r2416.bin
  flash:/diagfile/
  flash:/ifindex.dat
  flash:/startup.cfg
  flash:/startup.mdb
  flash:/lauth.dat
  flash:/license/
  flash:/logfile/
  flash:/pki/
  flash:/seclog/
  flash:/versionInfo/

<Comware7>copy flash:/5900_5920-CMW710-R2311P05.ipe ?
  STRING        [drive][path][file name]
  flash:        Device name
  ftp:          File on the FTP server
  slot1#flash:  Device name
  slot1#usba0:  Device name
  tftp:         File on the TFTP server
  usba0:        Device name

<Comware7>copy flash:/5900_5920-CMW710-R2311P05.ipe usba0:?
  usba0:/

<Comware7>copy flash:/5900_5920-CMW710-R2311P05.ipe usba0:/?
  "usba0:/System Volume Information/"
  usba0:/5900_5920-CMW710-R2416.ipe
  usba0:/5900_5920-cmw710-boot-r2311p05.bin
  usba0:/5900_5920-cmw710-boot-r2416.bin
  usba0:/5900_5920-cmw710-system-r2311p05.bin
  usba0:/5900_5920-cmw710-system-r2416.bin

<Comware7>copy flash:/5900_5920-CMW710-R2311P05.ipe usba0:/ ?
  <cr>

<Comware7>copy flash:/5900_5920-CMW710-R2311P05.ipe usba0:/


<Comware7>boot-loader ?
  file    Specify upgrade image files
  pex     Specify the startup software image files for PEXs to load from the
          parent device
  update  Update startup software images

<Comware7>boot-loader file ?
  boot    Specify a boot image file
  flash:  Device name
  usba0:  Device name

<Comware7>boot-loader file flash:/5900_5920-CMW710-R2311P05.ipe ?
  all   Set the startup software image for all the slot
  slot  Specify the slot

<Comware7>boot-loader file flash:/5900_5920-CMW710-R2311P05.ipe slot ?
  <1>  Slot number

<Comware7>boot-loader file flash:/5900_5920-CMW710-R2311P05.ipe slot 1 ?
  backup  Specify the packages as the backup startup software images
  main    Specify the packages as the main startup software images

<Comware7>boot-loader file flash:/5900_5920-CMW710-R2311P05.ipe slot 1 main ?
  <cr>
```

```
<Comware7>boot-loader file flash:/5900_5920-CMW710-R2311P05.ipe slot 1 main
```

Cisco

```
Cisco#show flash:

    2  -rwx         556  Mar 30 2011 00:07:35 -06:00  vlan.dat
  508  -rwx        2345  Aug 30 1993 00:54:39 -06:00  IPv6-3750E-1-base-12042014-1700.cfg
  509  -rwx    18586280  Mar 29 2011 20:09:52 -06:00  c3750e-universalk9-mz.150-1.SE.bin
  510  -rwx        2077  Feb 28 1993 18:14:58 -06:00  cisco-1-base-config-03052015-0010.cfg
  514  -rwx        4120  Feb 28 1993 18:02:19 -06:00  multiple-fs
  516  -rwx        2542  Feb 28 1993 18:02:18 -06:00  config.text
  517  -rwx        1915  Feb 28 1993 18:02:18 -06:00  private-config.text

57409536 bytes total (3827712 bytes free)

Cisco#show version
Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Version 15.0(1)SE
...
System image file is "flash:c3750e-universalk9-mz.150-1.SE.bin"
...

Cisco#copy ?
  /erase          Erase destination file system.
  /error          Allow to copy error file.
  /noverify       Don't verify image signature before reload.
  /verify         Verify image signature before reload.
  bs:             Copy from bs: file system
  cns:            Copy from cns: file system
  flash1:         Copy from flash1: file system
  flash:          Copy from flash: file system
  ftp:            Copy from ftp: file system
  http:           Copy from http: file system
  https:          Copy from https: file system
  logging         Copy logging messages
  null:           Copy from null: file system
  nvram:          Copy from nvram: file system
  rcp:            Copy from rcp: file system
  running-config  Copy from current system configuration
  scp:            Copy from scp: file system
  startup-config  Copy from startup configuration
  system:         Copy from system: file system
  tar:            Copy from tar: file system
  tftp:           Copy from tftp: file system
  tmpsys:         Copy from tmpsys: file system
  xmodem:         Copy from xmodem: file system
  ymodem:         Copy from ymodem: file system

Cisco#copy tftp:?
  tftp:  A URL beginning with this prefix

Cisco#copy tftp://10.0.100.111/c3750e-universalk9-mz.150-2.SE7.bin ?
  flash:          Copy to flash: file system
  null:           Copy to null: file system
  nvram:          Copy to nvram: file system
  running-config  Update (merge with) current system configuration
  startup-config  Copy to startup configuration
  syslog:         Copy to syslog: file system
  system:         Copy to system: file system
  tmpsys:         Copy to tmpsys: file system
  vb:             Copy to vb: file system

Cisco#copy tftp://10.0.100.111/c3750e-universalk9-mz.150-2.SE7.bin flash ?
  <cr>
```

```
Cisco#copy tftp://10.0.100.111/ c3750e-universalk9-mz.150-2.SE7.bin flash:
Destination filename [c3750e-universalk9-mz.150-2.SE7.bin]?


Cisco#copy scp:?
  scp:  A URL beginning with this prefix

Cisco#copy scp://10.0.100.111/c3750e-universalk9-mz.150-2.SE7.bin ?
  flash1:         Copy to flash1: file system
  flash:          Copy to flash: file system
  null:           Copy to null: file system
  nvram:          Copy to nvram: file system
  running-config  Update (merge with) current system configuration
  startup-config  Copy to startup configuration
  syslog:         Copy to syslog: file system
  system:         Copy to system: file system
  tmpsys:         Copy to tmpsys: file system

Cisco#copy scp://10.0.100.111/c3750e-universalk9-mz.150-2.SE7.bin flash ?
  <cr>

Cisco#copy scp://10.0.100.111/c3750e-universalk9-mz.150-2.SE7.bin flash
Source username [manager]? test
Destination filename [c3750e-universalk9-mz.150-2.SE7.bin]?


Cisco#copy xmodem: ?
  flash1:         Copy to flash1: file system
  flash:          Copy to flash: file system
  ftp:            Copy to ftp: file system
  http:           Copy to http: file system
  https:          Copy to https: file system
  null:           Copy to null: file system
  nvram:          Copy to nvram: file system
  rcp:            Copy to rcp: file system
  running-config  Update (merge with) current system configuration
  scp:            Copy to scp: file system
  startup-config  Copy to startup configuration
  syslog:         Copy to syslog: file system
  system:         Copy to system: file system
  tftp:           Copy to tftp: file system
  tmpsys:         Copy to tmpsys: file system
  vb:             Copy to vb: file system

Cisco#copy xmodem: flash: ?
  <cr>

Cisco#copy xmodem: flash:


Cisco#copy flash: ?
  flash1:         Copy to flash1: file system
  flash:          Copy to flash: file system
  ftp:            Copy to ftp: file system
  http:           Copy to http: file system
  https:          Copy to https: file system
  null:           Copy to null: file system
  nvram:          Copy to nvram: file system
  rcp:            Copy to rcp: file system
  running-config  Update (merge with) current system configuration
  scp:            Copy to scp: file system
  startup-config  Copy to startup configuration
```

```
  syslog:         Copy to syslog: file system
  system:         Copy to system: file system
  tftp:           Copy to tftp: file system
  tmpsys:         Copy to tmpsys: file system

Cisco#copy flash: tftp: ?
  <cr>

Cisco#copy flash: tftp:
Source filename []? c3750e-universalk9-mz.150-1.SE.bin
Address or name of remote host []? 10.0.100.111
Destination filename [c3750e-universalk9-mz.150-1.SE.bin]?


Cisco#copy flash: scp: ?
  <cr>

Cisco#copy flash: scp:
Source filename [c3750e-universalk9-mz.150-1.SE.bin]?
Address or name of remote host []? 10.0.100.111
Destination username [manager]? test
Destination filename [c3750e-universalk9-mz.150-1.SE.bin]?


Cisco(config)#boot system ?
  WORD    pathlist of boot file(s) ... file1;file2;...
  switch  Set system image for switches in the stack

Cisco(config)# boot system flash: c3750-advipservicesk9-mz.122-46.SE.bin ?
  <cr>

Cisco(config)# boot system flash: c3750-advipservicesk9-mz.122-46.SE.bin

Cisco(config)# license save file-sys://lic-location [switch switch-num]

Cisco(config)# license revoke permission-file-url output-rehost-ticket-url
```

Chapter 4 Configuration File Management

This chapter compares the commands used to manage configuration files on ArubaOS-Switch, Comware, and Cisco.

The ArubaOS-Switch operating system writes to or reads from specific areas of the file storage, depending on the commands you enter. Image files, configuration files, and local user ID and passwords are stored in separate/dedicated areas of flash. When you enter commands such as **copy** and **show**, the ArubaOS-Switch operating system writes to or reads from these dedicated areas of flash. (For more information, see the management and configuration guide for the HP ArubaOS-Switch ASIC switch you are managing.)

Comware and Cisco platforms use basic file systems. There are no dedicated areas in flash for specific files or file types. You are allowed to create subdirectories, and copy and move files just as you would on other "regular" file systems.

ArubaOS-Switch can store a maximum of three configuration files. Comware and Cisco switches can store potentially multiple configuration files; the only limitation is the amount of available flash memory on the switch file system.

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch# show running-config ?	<Comware>display current-configuration ?	Cisco#show running-config ?
	(Note: must save current configuration, then copy file accordingly)	
ArubaOS-Switch# copy running-config tftp 10.0.100.111 config2.cfg		Cisco#copy running-config tftp://10.0.100.111/Cisco.cfg
ArubaOS-Switch# copy running-config sftp 10.0.100.111 config2.cfg Attempting username/password authentication... Enter manager@10.0.100.111's password: ********		Cisco#copy running-config scp: Address or name of remote host []? 10.0.100.111 Destination username [manager]? Destination filename [cisco-confg]? Cisco.cfg Writing Cisco.cfg Password:
ArubaOS-Switch# copy running-config usb config2		
ArubaOS-Switch# copy running-config xmodem		
ArubaOS-Switch# copy startup-config tftp 10.0.100.111 ArubaOS-Switch_startup-config.cfg	<Comware>backup startup-configuration to 10.0.100.111 comware_startup-config.cfg	Cisco#copy startup-config tftp://10.0.100.111/Cisco_startup-config.cfg
ArubaOS-Switch# copy startup-config sftp 10.0.100.111 ArubaOS-Switch_startup-config.cfg		Cisco#copy startup-config scp: Address or name of remote host []? 10.0.100.111 Destination username

Attempting username/password authentication... Enter manager@10.0.100.111's password: ********		[manager]? Destination filename [cisco-confg]? Cisco_startup-config.cfg Writing Cisco_startup-config.cfg Password:
ArubaOS-Switch# copy config config1 config config2	<Comware>copy flash:/comware_main.cfg flash:/comware_main2.cfg	Cisco#copy flash:Cisco.cfg flash:Cisco_2.cfg
ArubaOS-Switch# copy config config1 tftp 10.0.100.111 config1.cfg	<Comware>tftp 10.0.100.111 put comware_main.cfg comware_startup-config.cfg	Cisco#copy flash:Cisco.cfg tftp://10.0.100.111/Cisco_2.cfg
ArubaOS-Switch# copy config config1 sftp 10.0.100.111 config1.cfg Attempting username/password authentication... Enter manager@10.0.100.111's password: ********	<Comware>sftp 10.0.100.111 Input Username: manager Trying 10.0.100.111 ... Press CTRL+K to abort Connected to 10.0.100.111 ... Enter password: sftp-client>put comware_main.cfg comware_startup-config.cfg sftp-client>bye	Cisco#copy flash:Cisco.cfg scp: Address or name of remote host []? 10.0.100.111 Destination username [manager]? Destination filename [Cisco.cfg]? Writing Cisco.cfg Password:
ArubaOS-Switch# erase startup-config	<Comware>reset saved-configuration main	Cisco#erase startup-config
ArubaOS-Switch# copy tftp startup-config 10.0.100.111 config6.cfg	<Comware>tftp 10.0.100.111 get comware_main.cfg startup.cfg	Cisco#copy tftp://10.0.100.111/Cisco_config3.cfg config.text
ArubaOS-Switch# copy sftp startup-config 10.0.100.111 config6.cfg Attempting username/password authentication... Enter manager@10.0.100.111's password: ********	<Comware>sftp 10.0.100.111 Input Username: manager Trying 10.0.100.111 ... Press CTRL+K to abort Connected to 10.0.100.111 ... Enter password: sftp-client>get comware_main.cfg startup.cfg sftp-client>bye	Cisco#copy scp: startup-config Address or name of remote host []? 10.0.100.111 Source username [manager]? Source filename []? Cisco_startup-config.cfg Destination filename [startup-config]? Password:
ArubaOS-Switch# copy tftp config config3 10.0.100.111 config3.cfg	<Comware>tftp 10.0.100.111 get comware_main3.cfg comware_main3.cfg	Cisco#copy tftp://10.0.100.111/Cisco_config2.cfg flash:Cisco_config2.cfg
ArubaOS-Switch# copy sftp config config3 10.0.100.111 config3.cfg Attempting username/password authentication... Enter manager@10.0.100.111's password: ********	<Comware>sftp 10.0.100.111 Input Username: manager Trying 10.0.100.111 ... Press CTRL+K to abort Connected to 10.0.100.111 ... Enter password: sftp-client>get comware_main3.cfg comware_main3.cfg sftp-client>bye	Cisco#copy scp: flash: Address or name of remote host []? 10.0.100.111 Source username [manager]? Source filename []? Cisco_config2.cfg Destination filename [Cisco_config2.cfg]? Password:
ArubaOS-Switch# show config files	<Comware>dir <Comware>display startup <Comware>display boot-loader	Cisco#show flash Cisco#show boot

ArubaOS-Switch# startup-default config config1	<Comware>startup saved-configuration comware_main.cfg main	Cisco(config)#boot config-file flash:Cisco.cfg
ArubaOS-Switch# startup-default primary config config1		
ArubaOS-Switch# boot system flash primary config config1		

ArubaOS-Switch

```
ArubaOS-Switch# show running-config
 change-history        Show the change-history logs of the running configuration.
 interface             Show the running configuration for interfaces.
 oobm                  Show the running configuration for OOBM.
 router                Show the running configuration for layer 3 protocols such as BGP,
                       OSPF, OSPFv3, PIM, RIP and VRRP.
 status                Show if the running configuration differs from the startup
                       configuration.
 structured            Show the running configuration in a grouped format.
 vlan                  Show the running configuration for VLANs.
 <cr>

ArubaOS-Switch# copy ?
command-output        Specify a CLI command to copy output of.
 config                Copy named configuration file.
 core-dump             Copy coredump file from flash.
 crash-data            Copy the switch crash data file.
 crash-log             Copy the switch log file.
 default-config        Copy custom default configuration.
 event-log             Copy event log file.
 fdr-log               Copy FDR logs from the switch to TFTP server, USB or xmodem
                       terminal.
 flash                 Copy the switch system image file.
 running-config        Copy running configuration file.
 sftp                  Copy data from a SFTP server.
 ssh-client-known-h... Copy the known hosts file.
 ssh-server-pub-key    Copy the switch's SSH server public key.
 startup-config        Copy in-flash configuration file.
 tftp                  Copy data from a TFTP server.
 usb                   Copy data from a USB flash drive.
 xmodem                Use xmodem on the terminal as the data source.

ArubaOS-Switch# copy running-config ?
 sftp                  Copy data to an SFTP server
 tftp                  Copy data to a TFTP server.
 usb                   Copy data to a USB flash drive.
 xmodem                Use xmodem on the terminal as the data destination.

ArubaOS-Switch# copy running-config tftp ?
 HOST-NAME-STR         Specify hostname of the TFTP server.
 IP-ADDR               Specify TFTP server IPv4 address.
 IPV6-ADDR             Specify TFTP server IPv6 address.

ArubaOS-Switch# copy running-config tftp 10.0.100.111 ?
 FILENAME-STR          Specify filename for the TFTP transfer.

ArubaOS-Switch# copy running-config tftp 10.0.100.111 config2.cfg ?
 oobm                  Use the OOBM interface to reach TFTP server.
```

```
 pc                     Change CR/LF to PC style.
 unix                   Change CR/LF to unix style.
 <cr>

ArubaOS-Switch# copy running-config tftp 10.0.100.111 config2.cfg

ArubaOS-Switch# copy running-config sftp ?
HOST-NAME-STR         Specify hostname of the SFTP server.
 IP-ADDR                Specify SFTP server IPv4 address.
 IPV6-ADDR              Specify SFTP server IPv6 address.
 user                   Specify the username on the remote system
 USERNAME@IP-STR        Specify the username along with remote system information
                        (hostname, IPv4 or IPv6 address).

ArubaOS-Switch# copy running-config sftp 10.0.100.111 ?
 FILENAME-STR           Specify filename for the SFTP transfer
 port                   TCP port of the SSH server on the remote system.

ArubaOS-Switch# copy running-config sftp 10.0.100.111 config2.cfg ?
 <cr>

ArubaOS-Switch# copy running-config sftp 10.0.100.111 config2.cfg
Attempting username/password authentication...
Enter manager@10.0.100.111's password: ********
SFTP download in progress.

ArubaOS-Switch# copy running-config usb ?
 FILENAME-STR           Specify filename for the USB transfer.

ArubaOS-Switch# copy running-config usb config2

ArubaOS-Switch# copy running-config xmodem ?
 pc                     Change CR/LF to PC style.
 unix                   Change CR/LF to unix style.
 <cr>

ArubaOS-Switch# copy running-config xmodem
Press 'Enter' and start XMODEM on your host...


ArubaOS-Switch# copy startup-config
 default-config         Copy source file to custom default configuration.
 sftp                   Copy data to an SFTP server
 tftp                   Copy data to a TFTP server.
 usb                    Copy data to a USB flash drive.
 xmodem                 Use xmodem on the terminal as the data destination.

ArubaOS-Switch# copy startup-config default-config ?
 <cr>
ArubaOS-Switch# copy startup-config default-config

ArubaOS-Switch# copy startup-config tftp ?
 HOST-NAME-STR          Specify hostname of the TFTP server.
 IP-ADDR                Specify TFTP server IPv4 address.
 IPV6-ADDR              Specify TFTP server IPv6 address.

ArubaOS-Switch# copy startup-config tftp 10.0.100.111 ?
 FILENAME-STR           Specify filename for the TFTP transfer.

ArubaOS-Switch# copy startup-config tftp 10.0.100.111 ArubaOS-Switch_startup-config.cfg

ArubaOS-Switch# copy startup-config sftp ?
 HOST-NAME-STR          Specify hostname of the SFTP server.
```

```
 IP-ADDR                Specify SFTP server IPv4 address.
 IPV6-ADDR              Specify SFTP server IPv6 address.
 user                   Specify the username on the remote system
 USERNAME@IP-STR        Specify the username along with remote system information
                        (hostname, IPv4 or IPv6 address).

ArubaOS-Switch# copy startup-config sftp 10.0.100.111 ?
 FILENAME-STR           Specify filename for the SFTP transfer
 port                   TCP port of the SSH server on the remote system.

ArubaOS-Switch# copy startup-config sftp 10.0.100.111 ArubaOS-Switch_startup.cfg ?
 oobm                   Use the OOBM interface to reach SFTP server.
 <cr>

ArubaOS-Switch# copy startup-config sftp 10.0.100.111 ArubaOS-Switch_startup.cfg
Attempting username/password authentication...
Enter manager@10.0.100.111's password: ********
SFTP download in progress.


ArubaOS-Switch# copy config ?
 config1
 config2

ArubaOS-Switch# copy config config1 ?
 config                 Copy data to the specified switch configuration file.
 default-config         Copy source file to custom default configuration.
 sftp                   Copy data to an SFTP server
 tftp                   Copy data to a TFTP server.
 usb                    Copy data to a USB flash drive.
 xmodem                 Use xmodem on the terminal as the data destination.

ArubaOS-Switch# copy config config1 config ?
 ASCII-STR              Enter an ASCII string for the 'config'
                        command/parameter.

ArubaOS-Switch# copy config config1 config config2 ?
<cr>

ArubaOS-Switch# copy config config1 config config2

ArubaOS-Switch# copy config config1 tftp 10.0.100.111 config1.cfg

ArubaOS-Switch# copy config config1 sftp 10.0.100.111 config1.cfg
Attempting username/password authentication...
Enter manager@10.0.100.111's password: ********
SFTP download in progress.


ArubaOS-Switch# erase startup-config ?
 <cr>

ArubaOS-Switch# erase startup-config
Configuration will be deleted and device rebooted, continue [y/n]?


ArubaOS-Switch# copy tftp startup-config 10.0.100.111 config6.cfg
Device may be rebooted, do you want to continue [y/n]?

ArubaOS-Switch# copy sftp startup-config 10.0.100.111 config6.cfg
Device may be rebooted, do you want to continue [y/n]?  y
Attempting username/password authentication...
Enter manager@10.0.100.111's password: ********
```

```
SFTP download in progress.

ArubaOS-Switch# copy tftp config config3 10.0.100.111 config3.cfg

ArubaOS-Switch# copy sftp config config3 10.0.100.111 config3.cfg
Attempting username/password authentication...
Enter manager@10.0.100.111's password: ********
SFTP download in progress.


ArubaOS-Switch# show config files
Configuration files:
 id | act pri sec | name
 ---+-------------+-------------------------------------------------
  1 |  *   *      | config1
  2 |          *  | config2
  3 |             | config3

ArubaOS-Switch# startup-default ?
 config                Specify configuration file to set as default.
 primary               Primary flash image.
 secondary             Secondary flash image.

ArubaOS-Switch# startup-default config ?
 config1
 config2
 config3
ArubaOS-Switch# startup-default config config1

ArubaOS-Switch# startup-default primary ?
 config                Specify configuration file to set as default.

ArubaOS-Switch# startup-default primary config ?
 config1
 config2
 config3

ArubaOS-Switch# startup-default primary config config1

ArubaOS-Switch# boot system ?
 flash                 Specify boot image to use after reboot.
 <cr>

ArubaOS-Switch# boot system flash ?
 primary               Primary flash image.
 secondary             Secondary flash image.

ArubaOS-Switch# boot system flash primary ?
 config                Specify configuration file to use on boot.
 <cr>

ArubaOS-Switch# boot system flash primary config ?
 config1
 config2
 config3

ArubaOS-Switch# boot system flash primary config config1 ?
 <cr>

ArubaOS-Switch# boot system flash primary config config1
```

Comware5

In this chapter, SFTP (Secure File Trasnfer Protocol) is used for secure file transfers. SCP (Secure Copy) is used in Chapter 3 for secure file transfers.

```
<Comware5>display current-configuration ?
  by-linenum     Display configuration with line number
  configuration  The pre-positive and post-positive configuration information
  exclude        Display current configuration without specified module
  interface      The interface configuration information
  |              Matching output
  <cr>

<Comware5>backup ?
  startup-configuration  Startup configuration

<Comware5>backup startup-configuration ?
  to  Indicate operation direction

<Comware5>backup startup-configuration to ?
  STRING<1-20>  IP address or hostname of TFTP Server

<Comware5>backup startup-configuration to 10.0.100.111 comware5_startup-config.cfg


<Comware5>copy ?
  STRING  [drive][path][file name]
  flash:  Device name

<Comware5>copy flash:/?
   flash:/comware_main.cfg
   flash:/startup.cfg
   flash:/startup1.cfg

<Comware5>copy flash:/comware_main.cfg ?
  STRING  [drive][path][file name]
  flash:  Device name

<Comware5>copy flash:/comware_main.cfg flash:/comware_main2.cfg ?
  <cr>

<Comware5>copy flash:/comware_main.cfg flash:/comware_main2.cfg


<Comware5>tftp ?
  STRING<1-20>  IP address or hostname of a remote system
  ipv6          IPv6 TFTP client

<Comware5>tftp 10.0.100.111 ?
  get   Download file from remote TFTP server
  put   Upload local file to remote TFTP server
  sget  Download securely from remote TFTP server

<Comware55>tftp 10.0.100.111 put ?
  STRING<1-135>  Source filename

<Comware5>tftp 10.0.100.111 put comware_main.cfg ?
  STRING<1-135>  Destination filename
  source         Specify a source
  vpn-instance   Specify a VPN instance
  <cr>
```

```
<Comware5>tftp 10.0.100.111 put comware_main.cfg comware_startup-config.cfg ?
  source  Specify a source
  <cr>

<Comware5>tftp 10.0.100.111 put comware_main.cfg comware_startup-config.cfg


<Comware5>sftp ?
  STRING<1-20>  IP address or hostname of remote system
  ipv6          Specify IPv6 address or hostname of remote system

<Comware5>sftp 10.0.100.111 ?
  INTEGER<0-65535>    Specified port number
  identity-key        Specify the algorithm for publickey authentication
  prefer-ctos-cipher  Specify the preferred encryption algorithm from client to
                      server
  prefer-ctos-hmac    Specify the preferred HMAC algorithm from client to
                      server
  prefer-kex          Specify the preferred key exchange algorithm
  prefer-stoc-cipher  Specify the preferred encryption algorithm from server to
                      client
  prefer-stoc-hmac    Specify the preferred HMAC algorithm from server to
                      client
  vpn-instance        Specify a VPN instance
  <cr>

<Comware5>sftp 10.0.100.111
Input Username: manager
Trying 10.0.100.111 ...
Press CTRL+K to abort
Connected to 10.0.100.111 ...
Enter password:

sftp-client>put comware_main.cfg comware_startup-config.cfg
Local file:comware_main.cfg --->  Remote file: /comware_startup-config.cfg
Uploading file successfully ended
sftp-client>bye
Bye
Connection closed.


<Comware5>reset saved-configuration ?
  backup  Backup config file
  main    Main config file
  <cr>

<Comware5>reset saved-configuration main ?
  backup  Backup config file
  main    Main config file
  <cr>

<Comware5>reset saved-configuration main


<Comware5>tftp 10.0.100.111 get comware_main.cfg startup.cfg

<Comware5>sftp 10.0.100.111
Input Username: manager
Trying 10.0.100.111 ...
Press CTRL+K to abort
Connected to 10.0.100.111 ...
Enter password:
```

```
sftp-client>get comware_main.cfg startup.cfg
Remote  file:/comware_main.cfg --->  Local file: startup.cfg.
Downloading file successfully ended
sftp-client>bye

<Comware5>tftp 10.0.100.111 get comware_main3.cfg comware_main3.cfg

<Comware5>sftp 10.0.100.111
Input Username: manager
Trying 10.0.100.111 ...
Press CTRL+K to abort
Connected to 10.0.100.111 ...
Enter password:

sftp-client>get comware_main3.cfg comware_main3.cfg
Remote  file:/comware_main3.cfg --->  Local file: comware_main3.cfg.
Downloading file successfully ended
sftp-client>bye


<Comware5>dir
Directory of flash:/

   0     -rw-      3816  Mar 06 2015 00:31:44   startup.cfg
   1     -rw-      8322  Feb 19 2015 17:04:50   config.cwmp
   2     drw-         -  Apr 26 2000 12:00:21   seclog
   3     -rw-    483732  Jan 23 2015 12:38:11   a5500ei-btm-721.btm
   4     -rw-       151  Mar 06 2015 00:31:39   system.xml
   5     -rw-      3816  Mar 09 2015 18:23:03   comware_main.cfg
   6     -rw-      3816  Mar 09 2015 18:17:41   comware_main2.cfg
   7     -rw-      3816  Mar 09 2015 18:24:02   comware_main3.cfg
   8     -rw-      4096  Nov 10 2012 02:44:37   comware5_dhcp.txt
   9     -rw-  14274135  Jan 23 2015 13:10:35   a5500ei-cmw520-r2221p07.bin
```

(will need to view files to determine which are configuration files)

```
<Comware5>display startup
MainBoard:
 Current startup saved-configuration file: flash:/startup.cfg
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: NULL
 Bootrom-access enable state: enabled

<Comware5>display boot-loader
 Slot 1
The current boot app is:  flash:/a5500ei-cmw520-r2221p07.bin
The main boot app is:     flash:/a5500ei-cmw520-r2221p07.bin
The backup boot app is:   flash:/a5500ei-cmw520-r2215.bin


<Comware5>startup ?
  bootrom-access       Bootrom access control
  saved-configuration  Saved-configuration file for starting system

<Comware5>startup saved-configuration ?
  comware_main.cfg
  comware_main2.cfg
  comware_main3.cfg
  startup.cfg

<Comware5>startup saved-configuration comware_main.cfg ?
  backup  Backup config file
  main    Main config file
```

```
  <cr>

<Comware5>startup saved-configuration comware_main.cfg main ?
  <cr>

<Comware5>startup saved-configuration Comware_main.cfg main
```

Comware7

In this chapter, SFTP (Secure File Trasnfer Protocol) is used for secure file transfers. SCP (Secure Copy) is used in Chapter 3 for secure file transfers.

```
<Comware7>display current-configuration ?
  >              Redirect it to a file
  >>             Redirect it to a file in append mode
  configuration  The pre-positive and post-positive configuration information
  diff           Display the differences between the current configuration and
                 the next-startup configuration
  interface      The interface configuration information
  |              Matching output
  <cr>


<Comware7>backup ?
  startup-configuration  Startup configuration file

<Comware7>backup startup-configuration ?
  to  Indicate the operation direction

<Comware7>backup startup-configuration to ?
  STRING<1-253>  IP address or hostname of the TFTP server

<Comware7>backup startup-configuration to 10.0.100.111 ?
  STRING<1-256>  Destination filename with the suffix .cfg
  <cr>

<Comware7>backup startup-configuration to 10.0.100.111 comware7_startup-config.cfg ?
  <cr>

<Comware7>backup startup-configuration to 10.0.100.111 comware7_startup-config.cfg


<Comware7>copy ?
  STRING        [drive][path][file name]
  flash:        Device name
  ftp:          File on the FTP server
  slot1#flash:  Device name
  slot1#usba0:  Device name
  tftp:         File on the TFTP server
  usba0:        Device name

<Comware7>copy flash:/?
  flash:/comware_main.cfg
  flash:/startup.cfg

<Comware7>copy flash:/comware_main.cfg ?
  STRING        [drive][path][file name]
  flash:        Device name
  ftp:          File on the FTP server
  slot1#flash:  Device name
  slot1#usba0:  Device name
  tftp:         File on the TFTP server
```

```
  usba0:        Device name

<Comware7>copy flash:/comware_main.cfg flash:/comware_main2.cfg ?
  <cr>

<Comware7>copy flash:/comware_main.cfg flash:/comware_main2.cfg


<Comware7>tftp ?
  STRING<1-253>  IP address or hostname of the TFTP Server
  ipv6           IPv6 TFTP Client

<Comware7>tftp 10.0.100.111 ?
  get   Download a file from the TFTP server
  put   Upload a local file to the TFTP server
  sget  Download a file from the TFTP server securely

<Comware7>tftp 10.0.100.111 put ?
  STRING<1-255>  Source filename

<Comware7>tftp 10.0.100.111 put comware_main.cfg ?
  STRING<1-255>  Destination filename
  dscp           Set the Differentiated Services Codepoint (DSCP) value
  source         Specify the source address for outgoing TFTP packets
  vpn-instance   Specify a VPN instance
  <cr>

<Comware7>tftp 10.0.100.111 put comware_main.cfg comware7_startup-config.cfg ?
  dscp          Set the Differentiated Services Codepoint (DSCP) value
  source        Specify the source address for outgoing TFTP packets
  vpn-instance  Specify a VPN instance
  <cr>

<Comware7>tftp 10.0.100.111 put comware_main.cfg comware7_startup-config.cfg


<Comware7>sftp ?
  STRING<1-253>  IP address or hostname of remote system
  ipv6           IPv6 information

<Comware7>sftp 10.0.100.111 ?
  INTEGER<1-65535>    Specify port number
  dscp                Set the Differentiated Services Codepoint (DSCP) value
  identity-key        Specify the algorithm for publickey authentication
  prefer-compress     Specify the preferred compression algorithm
  prefer-ctos-cipher  Specify the preferred encryption algorithm from client to
                      server
  prefer-ctos-hmac    Specify the preferred HMAC algorithm from client to server
  prefer-kex          Specify the preferred key exchange algorithm
  prefer-stoc-cipher  Specify the preferred encryption algorithm from server to
                      client
  prefer-stoc-hmac    Specify the preferred HMAC algorithm from server to client
  publickey           Specify the public key of server
  source              Specify a source
  vpn-instance        Specify a VPN instance
  <cr>

<Comware7>sftp 10.0.100.111
Username: manager
Press CTRL+C to abort.
Connecting to 10.0.100.111 port 22.
manager@10.0.100.111's password:
sftp> put comware_main.cfg comware7_startup-config.cfg
```

```
Uploading comware_main.cfg to /comware7_startup-config.cfg
comware_main.cfg                              100% 6787     6.6KB/s   00:00
sftp> bye


<Comware7>reset saved-configuration ?
  backup  Backup config file
  main    Main config file
  <cr>

<Comware7>reset saved-configuration main ?
  backup  Backup config file
  main    Main config file
  <cr>

<Comware7>reset saved-configuration main


<Comware7>tftp 10.0.100.111 get comware_main.cfg startup.cfg

<Comware7>sftp 10.0.100.111
Username: manager
Press CTRL+C to abort.
Connecting to 10.0.100.111 port 22.
manager@10.0.100.111's password:

sftp> get comware_main.cfg startup.cfg
Fetching /comware_main.cfg to startup.cfg
/comware_main.cfg                             100% 3816     3.7KB/s   00:00
sftp> bye


<Comware7>tftp 10.0.100.111 get comware_main3.cfg comware_main3.cfg

<Comware7>sftp 10.0.100.111
Username: manager
Press CTRL+C to abort.
Connecting to 10.0.100.111 port 22.
manager@10.0.100.111's password:

sftp> get comware7_main3.cfg comware7_main3.cfg
Fetching /comware7_main3.cfg to comware7_main.cfg
/comware7_main3.cfg                           100% 6787     6.6KB/s   00:00
sftp> bye


<Comware7>dir
Directory of flash:
   1 -rw-    61579264 Mar 25 2015 17:28:50   5900_5920-CMW710-R2311P05.ipe
   2 -rw-    10986496 Feb 04 2015 17:52:26   5900_5920-cmw710-boot-r2416.bin
   3 -rw-    66350080 Feb 04 2015 17:54:43   5900_5920-cmw710-system-r2416.bin
   4 -rw-        6787 Mar 25 2015 23:51:59   comware7_main.cfg
   5 -rw-        6787 Mar 25 2015 23:26:11   comware7_main2.cfg
   6 -rw-        6787 Mar 25 2015 23:26:11   comware7_main3.cfg
   7 drw-           - Dec 31 2010 18:00:23   diagfile
   8 -rw-        1580 Mar 25 2015 23:18:15   ifindex.dat
   9 -rw-           0 Oct 06 2014 12:02:16   lauth.dat
  10 drw-           - Dec 31 2010 18:00:24   license
  11 drw-           - Jan 01 2011 18:00:23   logfile
  12 drw-           - Sep 15 2014 10:45:45   pki
  13 drw-           - Dec 31 2010 18:00:23   seclog
  14 -rw-        6787 Mar 25 2015 23:18:16   startup.cfg
  15 -rw-      172286 Mar 25 2015 23:18:17   startup.mdb
```

```
  16 -rw-        3816 Mar 25 2015 23:49:12   startup1.cfg
  17 drw-           - Feb 04 2015 18:00:57   versionInfo
```

(will need to view files to determine which are configuration files)

```
<Comware7>display startup
MainBoard:
 Current startup saved-configuration file: flash:/startup.cfg
 Next main startup saved-configuration file: flash:/comware_main.cfg
 Next backup startup saved-configuration file: NULL

<Comware7>display boot-loader
Software images on slot 1:
Current software images:
  flash:/5900_5920-cmw710-boot-r2416.bin
  flash:/5900_5920-cmw710-system-r2416.bin
Main startup software images:
  flash:/5900_5920-cmw710-boot-r2416.bin
  flash:/5900_5920-cmw710-system-r2416.bin
Backup startup software images:
  None


<Comware7>startup ?
  saved-configuration  Saved-configuration file for starting system

<Comware7>startup saved-configuration ?
  comware7_main.cfg
  comware7_main2.cfg
  comware7_main3.cfg
  startup.cfg
  startup1.cfg

<Comware7>startup saved-configuration comware7_main.cfg ?
  backup  Backup configuration file
  main    Main configuration file
  <cr>

<Comware7>startup saved-configuration comware7_main.cfg main ?
  <cr>

<Comware7>startup saved-configuration comware7_main.cfg main
```

Cisco

```
Cisco#show running-config ?
  all         Configuration with defaults
  brief       configuration without certificate data
  class-map   Show class-map information
  flow        Global Flow configuration subcommands
  full        full configuration
  identity    Show identity profile/policy information
  interface   Show interface configuration
  linenum     Display line numbers in output
  map-class   Show map class information
  partition   Configuration corresponding a partition
  policy-map  Show policy-map information
  view        View options
  vlan        Show L2 VLAN information
  vrf         Show VRF aware configuration
  |           Output modifiers
  <cr>

Cisco#copy ?
```

```
  /erase          Erase destination file system.
  /error          Allow to copy error file.
  /noverify       Don't verify image signature before reload.
  /verify         Verify image signature before reload.
  bs:             Copy from bs: file system
  cns:            Copy from cns: file system
  flash1:         Copy from flash1: file system
  flash:          Copy from flash: file system
  ftp:            Copy from ftp: file system
  http:           Copy from http: file system
  https:          Copy from https: file system
  logging         Copy logging messages
  null:           Copy from null: file system
  nvram:          Copy from nvram: file system
  rcp:            Copy from rcp: file system
  running-config  Copy from current system configuration
  scp:            Copy from scp: file system
  startup-config  Copy from startup configuration
  system:         Copy from system: file system
  tar:            Copy from tar: file system
  tftp:           Copy from tftp: file system
  tmpsys:         Copy from tmpsys: file system
  xmodem:         Copy from xmodem: file system
  ymodem:         Copy from ymodem: file system

Cisco#copy running-config ?
  flash1:         Copy to flash1: file system
  flash:          Copy to flash: file system
  ftp:            Copy to ftp: file system
  http:           Copy to http: file system
  https:          Copy to https: file system
  null:           Copy to null: file system
  nvram:          Copy to nvram: file system
  rcp:            Copy to rcp: file system
  running-config  Update (merge with) current system configuration
  scp:            Copy to scp: file system
  startup-config  Copy to startup configuration
  syslog:         Copy to syslog: file system
  system:         Copy to system: file system
  tftp:           Copy to tftp: file system
  tmpsys:         Copy to tmpsys: file system

Cisco#copy running-config tftp://10.0.100.111/Cisco.cfg
Address or name of remote host [10.0.100.111]?
Destination filename [Cisco.cfg]?

Cisco#copy running-config scp:
Address or name of remote host []? 10.0.100.111
Destination username [manager]?
Destination filename [cisco-confg]? Cisco.cfg
Writing Cisco.cfg
Password:

Cisco#copy startup-config ?
  flash1:         Copy to flash1: file system
  flash:          Copy to flash: file system
  ftp:            Copy to ftp: file system
  http:           Copy to http: file system
  https:          Copy to https: file system
  null:           Copy to null: file system
  nvram:          Copy to nvram: file system
  rcp:            Copy to rcp: file system
  running-config  Update (merge with) current system configuration
```

```
  scp:            Copy to scp: file system
  startup-config  Copy to startup configuration
  syslog:         Copy to syslog: file system
  system:         Copy to system: file system
  tftp:           Copy to tftp: file system
  tmpsys:         Copy to tmpsys: file system

Cisco#copy startup-config tftp://10.0.100.111/Cisco_startup-config.cfg
Address or name of remote host [10.0.100.111]?
Destination filename [Cisco_startup-config]?

Cisco#copy startup-config scp:
Address or name of remote host []? 10.0.100.111
Destination username [manager]?
Destination filename [cisco-confg]? Cisco_startup-config.cfg
Writing Cisco_startup-config.cfg
Password:


Cisco#copy flash:?
flash:Cisco.cfg
flash:config.text
flash:info
flash:multiple-fs
flash:private-config.text
flash:vlan.dat

Cisco#copy flash:Cisco.cfg ?
  flash1:         Copy to flash1: file system
  flash:          Copy to flash: file system
  ftp:            Copy to ftp: file system
  http:           Copy to http: file system
  https:          Copy to https: file system
  null:           Copy to null: file system
  nvram:          Copy to nvram: file system
  rcp:            Copy to rcp: file system
  running-config  Update (merge with) current system configuration
  scp:            Copy to scp: file system
  startup-config  Copy to startup configuration
  syslog:         Copy to syslog: file system
  system:         Copy to system: file system
  tftp:           Copy to tftp: file system
  tmpsys:         Copy to tmpsys: file system

Cisco#copy flash:Cisco.cfg flash:Cisco_2.cfg

Cisco#copy flash:Cisco.cfg tftp://10.0.100.111/Cisco_2.cfg
Address or name of remote host [10.0.100.111]?
Destination filename [Cisco_2.cfg]?

Cisco#copy flash:Cisco.cfg scp:
Address or name of remote host []? 10.0.100.111
Destination username [manager]?
Destination filename [Cisco.cfg]?
Writing Cisco.cfg
Password:

Cisco#erase startup-config

Cisco#copy tftp://10.0.100.111/Cisco_config3.cfg config.text
Destination filename [config.text]?
Accessing tftp://10.0.100.111/Cisco_config3.cfg...
```

```
Cisco#copy scp: ?
  flash1:         Copy to flash1: file system
  flash:          Copy to flash: file system
  null:           Copy to null: file system
  nvram:          Copy to nvram: file system
  running-config  Update (merge with) current system configuration
  startup-config  Copy to startup configuration
  syslog:         Copy to syslog: file system
  system:         Copy to system: file system
  tmpsys:         Copy to tmpsys: file system

Cisco#copy scp: startup-config
Address or name of remote host []? 10.0.100.111
Source username [manager]?
Source filename []? Cisco_startup-config.cfg
Destination filename [startup-config]?

Password:

Cisco#copy tftp://10.0.100.111/Cisco_config2.cfg flash:Cisco_config2.cfg
Destination filename [Cisco_config2.cfg]?


Cisco#copy scp: flash:
Address or name of remote host []? 10.0.100.111
Source username [manager]?
Source filename []? Cisco_config2.cfg
Destination filename [Cisco_config2.cfg]?

Password:


Cisco#show flash:
Directory of flash:/

    2  -rwx    11135796   Mar 1 1993 00:10:48 +00:00  c3750-advipservicesk9-mz.122-46.SE.bin
    7  -rwx        2019   Mar 9 1993 07:30:27 +00:00  config.text
    8  -rwx        2019   Mar 9 1993 07:25:59 +00:00  Cisco.cfg
   11  -rwx        2019   Mar 9 1993 07:26:51 +00:00  Cisco2.cfg

(will need to view files to determine which are configuration files)

Cisco#show boot
BOOT path-list      : flash:/c3750e-universalk9-mz.150-1.SE.bin
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break        : no
Manual Boot         : no
HELPER path-list    :
Auto upgrade        : yes
Auto upgrade path   :
NVRAM/Config file
      buffer size:   524288
Timeout for Config
          Download:    0 seconds
Config Download
       via DHCP:       disabled (next boot: disabled)


Cisco(config)#boot ?
  auto-copy-sw         enable auto-copy of compatible software to stack members
                       that have joined the stack in version-mismatch mode
```

```
  auto-download-sw     url specifying pathname used for automatic software
                       upgrades
  boothlpr             Boot Helper System Image
  buffersize           Specify the buffer size for filesystem-simulated NVRAM
  config-file          Configuration File
  enable-break         Enable Break while booting
  helper               Helper Image(s)
  helper-config-file   Helper Configuration File
  host                 Router-specific config file
  manual               Manual Boot
  private-config-file  Private Configuration File
  system               System Image
  time                 Set the boot time of a switch

Cisco(config)#boot config-file ?
  WORD  config file name

Cisco(config)#boot config-file flash:Cisco.cfg
```

Chapter 5 Syslog Services

This chapter compares the commands used to configure syslog services, such as the syslog server's IP address and the logging facility.

Syslog is a client-server logging tool that allows a client switch to send event notification messages to a networked device operating with Syslog server software. Syslog can store these messages in a file for later debugging analysis.

To use the Syslog feature, you must install and configure a Syslog server application on a networked host accessible to the switch.

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# logging 10.0.100.111	[Comware]info-center loghost 10.0.100.111	Cisco(config)#logging 10.0.100.111
ArubaOS-Switch(config)# logging facility ?	[Comware]info-center loghost 10.0.100.111 facility ?	Cisco(config)#logging facility ?
ArubaOS-Switch(config)# logging severity ?		Cisco(config)#logging console ?
	[Comware]info-center timestamp loghost date	Cisco(config)#service timestamps log datetime localtime
ArubaOS-Switch# show logging ?	[Comware]display logbuffer ?	Cisco#show logging ?

ArubaOS-Switch

```
ArubaOS-Switch(config)# logging ?
 facility              Specify the syslog facility value that will be used for all syslog
                       servers.
 filter                Create a filter to restrict which events are logged.
 IP-ADDR               Add an IPv4 address to the list of receiving syslog servers.
 IPV6-ADDR             Add an IPv6 address to the list of receiving syslog servers.
 notify                Notification of the specified type will be sent to the syslog
                       server(s).
 origin-id             Specify the origin information for the syslog message.
 priority-descr        A text string associated with the values of facility, severity,
                       and system-module.
 severity              Event messages of the specified severity or higher will be sent to
                       the syslog server.
 system-module         Event messages of the specified system module (subsystem) will be
                       sent to the syslog server.

ArubaOS-Switch(config)# logging 10.0.100.111 ?
 control-descr         A text string associated with the given IP-ADDr.
 oobm                  Add an IP address to the list of receiving Syslog servers.
 udp                   Use UDP as the transport protocol (default UDP port #: 514)
 tcp                   Use TCP as the transport protocol (default TCP port #: 1470)
 tls                   Use TLS as the transport protocol (default TLS port #: 6514)
 <cr>

ArubaOS-Switch(config)# logging 10.0.100.111

ArubaOS-Switch(config)# logging facility ?
 kern
 user
```

```
 mail
 daemon
 auth
 syslog
 lpr
 news
 uucp
 sys9
 sys10
 sys11
 sys12
 sys13
 sys14
 cron
 local0
 local1
 local2
 local3
 local4
 local5
 local6
 local7

ArubaOS-Switch(config)# logging severity ?
 major
 error
 warning
 info
 debug


ArubaOS-Switch# show logging ?
 -a                    Display all log events, including those from previous boot cycles.
 -b                    Display log events as time since boot instead of date/time format.
 -r                    Display log events in reverse order (most recent first).
 -s                    Display commander and standby commander log events.
 -t                    Display log events in granularity in 10 milli seconds.
 -m                    Major event class.
 -e                    Error event class.
 -p                    Performance event class.
 -w                    Warning event class.
 -i                    Information event class.
 -d                    Debug event class.
 filter                Display log filter configuration and status information.
 OPTION-STR            Filter events shown.
 <cr>
```

Comware5

```
[Comware5]info-center ?
  channel           Specify the name of information channel
  console           Settings of console configuration
  enable            Enable the information center
  format            Format of syslog message
  logbuffer         Settings of logging buffer configuration
  loghost           Settings of logging host configuration
  monitor           Settings of monitor configuration
  security-logfile  Specify security log file configuration
  snmp              Settings of snmp configuration
  source            Informational source settings
  synchronous       Synchronize info-center output
  syslog            Setting of syslog configuration
  timestamp         Set the time stamp type of information
  trapbuffer        Settings of trap buffer configuration
```

```
[Comware5]info-center loghost ?
  STRING<1-255>  Logging host ip address or hostname
  ipv6           Specify an IPv6 address
  source         Set the source address of packets sent to loghost
  vpn-instance   Specify a VPN instance

[Comware5]info-center loghost 10.0.100.111 ?
  channel   Assign channel to the logging host
  dscp      Differentiated Services Code Point (DSCP)
  facility  Set logging host facility
  port      Assign port number to the logging host
  <cr>

[Comware5]info-center loghost 10.0.100.111

[Comware5]info-center loghost 10.0.100.111 facility ?
  local0  Logging host facility
  local1  Logging host facility
  local2  Logging host facility
  local3  Logging host facility
  local4  Logging host facility
  local5  Logging host facility
  local6  Logging host facility
  local7  Logging host facility

[Comware5]info-center timestamp ?
  debugging  Set the time stamp type of the debug information
  log        Set the time stamp type of the log information
  loghost    Set the time stamp type of the information to loghost
  trap       Set the time stamp type of the alarm information

[Comware5]info-center timestamp loghost ?
  date          Information time stamp of date type
  iso           Information time stamp of format in ISO 8601
  no-year-date  Information time stamp of date without year type
  none          None information time stamp

[Comware5]info-center timestamp loghost date ?
  <cr>

[Comware5]info-center timestamp loghost date


[Comware5]display logbuffer ?
  level    Only show items whose level match the designated level
  reverse  Display entries chronologically, with the most recent entry at the
           top
  size     Limit display to the most recent specified number of events
  slot     Only show items which are from the designated slot
  summary  A summary of the logging buffer
  |        Output modifiers
  <cr>
```

Comware7

```
[Comware7]info-center ?
  diagnostic-logfile  Diagnostic log file configuration
  enable              Enable the information center
  format              Format of syslog message
  logbuffer           Log buffer configuration
  logfile             Log file configuration
  logging             Specify log configuration
  loghost             Log host configuration
```

```
  security-logfile    Security log file configuration
  source              Informational source settings
  synchronous         Enable synchronous information output
  syslog              Setting of syslog configuration
  timestamp           Set the time stamp format of the log
  trace-logfile       Trace log file configuration

[Comware7]info-center loghost ?
  STRING<1-253>  Hostname of the log host
  X.X.X.X        IP address of the log host
  ipv6           Specify an IPv6 log host
  source         Specify the source IP address for log information
  vpn-instance   Specify the VPN instance to which the log host belongs

[Comware7]info-center loghost 10.0.100.111 ?
  facility  Specify the logging facility of the log host
  port      Specify the port number of the log host
  <cr>

[Comware7]info-center loghost 10.0.100.111

[Comware7]info-center loghost 10.0.100.111 facility ?
  local0  Set the logging facility to local0
  local1  Set the logging facility to local1
  local2  Set the logging facility to local2
  local3  Set the logging facility to local3
  local4  Set the logging facility to local4
  local5  Set the logging facility to local5
  local6  Set the logging facility to local6
  local7  Set the logging facility to local7

[Comware7]info-center timestamp ?
  boot     The time taken to boot up the system
  date     The current system date and time
  loghost  Log host configuration
  none     No time information is provided

[Comware7]info-center timestamp loghost ?
  date          The current system date and time
  iso           Set the time stamp to ISO 8601 format
  no-year-date  The current system date and time (year exclusive)
  none          No time information is provided

[Comware7]info-center timestamp loghost date ?
  <cr>

[Comware7]info-center timestamp loghost date


[Comware7]display logbuffer ?
  >        Redirect it to a file
  >>       Redirect it to a file in append mode
  level    Display log entries with the specified severity level
  reverse  Display log entries chronologically, with the most recent entry at
           the top
  size     Display specified number of log entries
  slot     Specify the slot number
  summary  Display summary information of the log buffer
  |        Matching output
  <cr>
```

Cisco

```
Cisco(config)#logging ?
```

```
  Hostname or A.B.C.D  IP address of the logging host
  buffered             Set buffered logging parameters
  buginf               Enable buginf logging for debugging
  cns-events           Set CNS Event logging level
  console              Set console logging parameters
  count                Count every log message and timestamp last occurance
  delimiter            Append delimiter to syslog messages
  discriminator        Create or modify a message discriminator
  esm                  Set ESM filter restrictions
  exception            Limit size of exception flush output
  facility             Facility parameter for syslog messages
  file                 Set logging file parameters
  filter               Specify logging filter
  history              Configure syslog history table
  host                 Set syslog server IP address and parameters
  message-counter      Configure log message to include certain counter value
  monitor              Set terminal line (monitor) logging parameters
  on                   Enable logging to all enabled destinations
  origin-id            Add origin ID to syslog messages
  persistent           Set persistent logging parameters
  queue-limit          Set logger message queue size
  rate-limit           Set messages per second limit
  reload               Set reload logging level
  server-arp           Enable sending ARP requests for syslog servers when
                       first configured
  smartlog             Smartlog Global Configuration Commands
  source-interface     Specify interface for source address in logging
                       transactions
  trap                 Set syslog server logging level
  userinfo             Enable logging of user info on privileged mode enabling

Cisco(config)#logging 10.0.100.111


Cisco(config)#logging facility ?
  auth    Authorization system
  cron    Cron/at facility
  daemon  System daemons
  kern    Kernel
  local0  Local use
  local1  Local use
  local2  Local use
  local3  Local use
  local4  Local use
  local5  Local use
  local6  Local use
  local7  Local use
  lpr     Line printer system
  mail    Mail system
  news    USENET news
  sys10   System use
  sys11   System use
  sys12   System use
  sys13   System use
  sys14   System use
  sys9    System use
  syslog  Syslog itself
  user    User process
  uucp    Unix-to-Unix copy system

Cisco(config)#logging console ?
  <0-7>          Logging severity level
  alerts         Immediate action needed           (severity=1)
```

```
  critical       Critical conditions               (severity=2)
  debugging      Debugging messages                (severity=7)
  discriminator  Establish MD-Console association
  emergencies    System is unusable                (severity=0)
  errors         Error conditions                  (severity=3)
  filtered       Enable filtered logging
  guaranteed     Guarantee console messages
  informational  Informational messages            (severity=6)
  notifications  Normal but significant conditions (severity=5)
  warnings       Warning conditions                (severity=4)
  xml            Enable logging in XML
  <cr>


Cisco(config)#service ?
  call-home              Enable call-home service
  compress-config        Compress the nvram configuration file
  config                 TFTP load config files
  counters               Control aging of interface counters
  dhcp                   Enable DHCP server and relay agent
  disable-ip-fast-frag   Disable IP particle-based fast fragmentation
  exec-callback          Enable exec callback
  exec-wait              Delay EXEC startup on noisy lines
  finger                 Allow responses to finger requests
  hide-telnet-addresses  Hide destination addresses in telnet command
  linenumber             enable line number banner for each exec
  nagle                  Enable Nagle's congestion control algorithm
  old-slip-prompts       Allow old scripts to operate with slip/ppp
  pad                    Enable PAD commands
  password-encryption    Encrypt system passwords
  password-recovery      Disable password recovery
  prompt                 Enable mode specific prompt
  pt-vty-logging         Log significant VTY-Async events
  sequence-numbers       Stamp logger messages with a sequence number
  slave-log              Enable log capability of slave IPs
  tcp-keepalives-in      Generate keepalives on idle incoming network
                         connections
  tcp-keepalives-out     Generate keepalives on idle outgoing network
                         connections
  tcp-small-servers      Enable small TCP servers (e.g., ECHO)
  telnet-zeroidle        Set TCP window 0 when connection is idle
  timestamps             Timestamp debug/log messages
  udp-small-servers      Enable small UDP servers (e.g., ECHO)

Cisco(config)#service timestamps ?
  debug  Timestamp debug messages
  log    Timestamp log messages
  <cr>

Cisco(config)#service timestamps log ?
  datetime  Timestamp with date and time
  uptime    Timestamp with system uptime
  <cr>

Cisco(config)#service timestamps log datetime ?
  localtime      Use local time zone for timestamps
  msec           Include milliseconds in timestamp
  show-timezone  Add time zone information to timestamp
  year           Include year in timestamp
  <cr>

Cisco(config)#service timestamps log datetime localtime ?
  msec           Include milliseconds in timestamp
```

```
  show-timezone  Add time zone information to timestamp
  year           Include year in timestamp
  <cr>

Cisco(config)#service timestamps log datetime localtime

Cisco#show logging ?
  count       Show counts of each logging message
  history     Show the contents of syslog history table
  onboard     Onboard logging information
  persistent  Show the contents of the logging persistent
  smartlog    Smartlog show commands
  xml         Show the contents of XML logging buffer
  |           Output modifiers
  <cr>
```

Chapter 6 Time Service

This chapter compares commands you can use to configure and synchronize the switch time with a trusted time source, using time protocols such as Network Time Protocol (NTP) and Simple NTP (SNTP).

Using time synchronization ensures a uniform time among interoperating devices. This helps to manage and troubleshoot switch operation by attaching meaningful time data to event and error messages.

a) NTP

ArubaOS-Switch	Comware5	Cisco
ArubaOS-Switch(config)# ntp server 10.0.100.251	[Comware5]ntp-service unicast-server 10.0.100.251	Cisco(config)#ntp server 10.0.100.251
ArubaOS-Switch(config)# ntp unicast		
ArubaOS-Switch(config)# timesync ntp		
ArubaOS-Switch(config)# ntp enable		
ArubaOS-Switch(config)# show ntp associations	[Comware5]display ntp-service sessions	Cisco#show ntp associations
ArubaOS-Switch# show ntp status	[Comware5]display ntp-service status	Cisco#show ntp status
		Cisco#show ntp status
ArubaOS-Switch(config)# clock timezone us central		Cisco(config)#clock timezone US-Cent -6
ArubaOS-Switch(config)# clock summer-time		
ArubaOS-Switch(config)# time daylight-time-rule continental-us-and-canada	[Comware5] clock summer-time US-Central one-off 02:00:00 03/08/2015 02:00:00 11/01/2015 01:0 0:00	Cisco(config)# clock summer-time US-Cent date mar 8 2015 02:00 nov 1 2015 02:00 60
ArubaOS-Switch# show time	[Comware5]display clock	Cisco#show clock Cisco#show clock detail
ArubaOS-Switch(config)#timesync ntp		Cisco(config)#feature ntp
ArubaOS-Switch(config)# ntp ipv6-multicast		Cisco(config)# ntp server {ip-address | ipv6-address | dns-name} [key key-id] [maxpoll max-poll] [minpoll min-poll] [prefer] [use-vrf vrf-name]
	Comware7	
	[Comware7]ntp-service unicast-server 10.0.100.251	
	[Comware7]ntp-service enable	
	[Comware7]display ntp-service sessions	
	[Comware7]display ntp-service status	
	[Comware7]clock timezone US-Central minus 06:00:00	

	[Comware7]clock summer-time US-Central 02:00:00 03/08 02:00:00 11/01 01:00:00	
	[Comware7]clock protocol ntp	
	[Comware7]display clock	

ArubaOS-Switch

```
ArubaOS-Switch(config)# ntp ?
 authentication        Configure NTP authentication.
 broadcast             Operate in broadcast mode.
 enable                Enable/disable NTP.
 max-association       Maximum number of Network Time Protocol (NTP) associations.
 server                Configure a NTP server to poll for time synchronization.
 trap                  Enable/disable NTP traps.
 unicast               Operate in unicast mode.

ArubaOS-Switch(config)# ntp server ?
 IP-ADDR               The IPv4 address of the server
 IPV6-ADDR             The IPv6 address of the server

ArubaOS-Switch(config)# ntp server 10.0.100.251 ?
 burst                 Enables burst mode.
 iburst                Enables initial burst (iburst) mode.
 key-id                Set the authentication key to use for this server.
 max-poll              Configures the maximum time intervals in seconds.
 min-poll              Configures the minimum time intervals in seconds.
 oobm                  Use the OOBM interface to connect to the server.
 <cr>

ArubaOS-Switch(config)# ntp server 10.0.100.251

ArubaOS-Switch(config)# ntp unicast ?
 <cr>

ArubaOS-Switch(config)# ntp unicast

ArubaOS-Switch(config)# timesync ?
 ntp                   Update the system clock using NTP.
 sntp                  Update the system clock using SNTP.
 timep                 Update the system clock using TIMEP.
 timep-or-sntp         Update the system clock using TIMEP or SNTP.

ArubaOS-Switch(config)# timesync ntp ?
 <cr>

ArubaOS-Switch(config)# timesync ntp


ArubaOS-Switch(config)# show ntp associations

                            NTP Associations Entries

 Remote           St   T    When   Poll  Reach    Delay    Offset   Dispersion
 --------------- ---- ---- ------ ----- -------- -------- -------- ----------
 10.0.100.251     2    u    497    6     177      0.000    0.000    8.02417

ArubaOS-Switch# show ntp status

 NTP Status Information
```

```
  NTP Status              : Enabled         NTP Mode        : Unicast
  Synchronization Status  : Synchronized    Peer Dispersion : 0.00000 sec
  Stratum Number          : 3               Leap Direction  : 0
  Reference Assoc ID      : 0               Clock Offset    : -490.51406 sec
  Reference ID            : 10.0.100.251    Root Delay      : 0.09215 sec
  Precision               : 2**-18          Root Dispersion : 490.54954 sec
  NTP Up Time             : 0d 0h 20m       Time Resolution : 440 nsec
  Drift                   : 0.00000 sec/sec

  System Time             : Wed Apr 27 17:43:49 2016
  Reference Time          : Wed Apr 27 16:21:27 2016


ArubaOS-Switch(config)# clock ?
 datetime              Specify the time and date
 set                   Set current time and/or date.
 summer-time           Enable/disable daylight-saving time changes.
 timezone              Set the number of hours your location is to the West(-) or East(+)
                       of GMT.
 <cr>

ArubaOS-Switch(config)# clock timezone ?
 gmt                   Number of hours your timezone is to the West(-) or East(+) of GMT.
 us                    Timezone for US locations.

ArubaOS-Switch(config)# clock timezone us
 alaska
 aleutian
 arizona
 central
 east_indiana
 eastern
 hawaii
 michigan
 mountain
 pacific
 samoa

ArubaOS-Switch(config)# clock timezone us central
 <cr>

ArubaOS-Switch(config)# clock summer-time
 <cr>


ArubaOS-Switch(config)# time ?
 begin-date            The begin date of daylight savings time
 MM/DD[/[YY]YY]        New date
 daylight-time-rule    The daylight savings time rule for your location
 end-date              The end date of daylight savings time
 HH:MM[:SS]            New time
 timezone              The number of minutes your location is West(-) or East(+) of GMT
 <cr>

ArubaOS-Switch(config)# time daylight-time-rule ?
 none
 alaska
 continental-us-and-canada
 middle-europe-and-portugal
 southern-hemisphere
 western-europe
 user-defined
```

```
ArubaOS-Switch(config)# time daylight-time-rule continental-us-and-canada ?
 begin-date            The begin date of daylight savings time
 MM/DD[/[YY]YY]        New date
 end-date              The end date of daylight savings time
 HH:MM[:SS]            New time
 timezone              The number of minutes your location is West(-) or East(+) of GMT
 <cr>

ArubaOS-Switch(config)# time daylight-time-rule continental-us-and-canada


ArubaOS-Switch# show time
Wed Apr 27 17:45:52 2016
```

Comware5

```
[Comware5]ntp-service ?
  access                NTP access control
  authentication        Authenticate NTP time source
  authentication-keyid  Specify NTP authentication keyid
  dscp                  Differentiated Services Codepoint (DSCP)
  max-dynamic-sessions  Specify the maximum connections
  reliable              Specify trusted keyid of NTP
  source-interface      Interface corresponding to sending NTP packet
  unicast-peer          Specify NTP peer
  unicast-server        Specify NTP server

[Comware5]ntp-service unicast-server ?
  STRING<1-20>  Host name of a remote system
  X.X.X.X       IP address
  vpn-instance  Specify VPN-Instance of MPLS VPN

[Comware5]ntp-service unicast-server 10.0.100.251 ?
  authentication-keyid  Specify authentication keyid
  priority              Prefer to this remote host if possible
  source-interface      Interface corresponding to sending NTP packet
  version               Specify NTP version
  <cr>

[Comware5]ntp-service unicast-server 10.0.100.251


[Comware5]display ntp-service ?
  sessions  NTP connection
  status    NTP status and configuration information
  trace     Trace the time synchronization information

<Comware5>dis ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**************************************************************************
[12345]10.0.100.251    216.218.192.202    2   255 1024   37    6.4    3.3    7.3
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1

[Comware5]display ntp-service status
 Clock status: synchronized
 Clock stratum: 12
 Reference clock ID: 10.0.100.251
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^18
 Clock offset: -1.1988 ms
 Root delay: 75.71 ms
 Root dispersion: 510.97 ms
```

```
 Peer dispersion: 500.41 ms
 Reference time: 21:15:29.197 UTC Mar 10 2015(D8A9DD71.3282E87D)


[Comware5]clock ?
  summer-time  Configure summer time
  timezone     Configure time zone

[Comware5]clock timezone ?
  STRING<1-32>  Name of time zone

[Comware5]clock timezone US-Central ?
  add    Add time zone offset
  minus  Minus time zone offset

[Comware5]clock timezone US-Central minus ?
  TIME  Time zone offset (HH:MM:SS)

[Comware5]clock timezone US-Central minus 06:00:00 ?
  <cr>

[Comware5]clock timezone US-Central minus 06:00:00


[Comware5]clock summer-time ?
  STRING<1-32>  Name of time zone in summer

[Comware5]clock summer-time US-Central ?
  one-off    Configure absolute summer time
  repeating  Configure recurring summer time

[Comware5]clock summer-time US-Central one-off ?
  TIME  Time to start (HH:MM:SS)

[Comware5]clock summer-time US-Central one-off 02:00:00 ?
  DATE  Date to start (MM/DD/YYYY or YYYY/MM/DD, valid year: 2000-2035)

[Comware5]clock summer-time US-Central one-off 02:00:00 03/08/2015 ?
  TIME  Time to end (HH:MM:SS)

[Comware5]clock summer-time US-Central one-off 02:00:00 03/08/2015 02:00:00 ?
  DATE  Date to end (MM/DD/YYYY or YYYY/MM/DD, valid year: 2000-2035)

[Comware5]clock summer-time US-Central one-off 02:00:00 03/08/2015 02:00:00 11/01/2015 ?
  TIME  Time added to the current system time (HH:MM:SS)

[Comware5]clock summer-time US-Central one-off 02:00:00 03/08/2015 02:00:00 11/01/2015 01:0
0:00 ?
  <cr>

[Comware5]clock summer-time US-Central one-off 02:00:00 03/08/2015 02:00:00 11/01/2015 01:0
0:00


[Comware5]display clock
16:26:54 US-Central Tue 03/10/2015
Time Zone : US-Central minus 06:00:00
Summer-Time : US-Central one-off 02:00:00 03/08/2015 02:00:00 11/01/2015  01:00:00
```

Comware7

```
[Comware7]ntp-service ?
  authentication        Configure NTP authentication
  authentication-keyid  Specify an authentication key ID
```

```
  dscp                   Set the Differentiated Services Codepoint (DSCP) value
  enable                 Enable NTP service
  ipv6                   IPv6 protocol
  max-dynamic-sessions   Specify the maximum number of dynamic NTP sessions
  peer                   Permit full access
  query                  Permit control query
  refclock-master        Configure the local clock as a master clock
  reliable               Specify a trusted key
  server                 Permit server access and query
  source                 Specify a source interface
  synchronization        Permit server access only
  unicast-peer           Specify a NTP peer
  unicast-server         Specify a NTP server

[Comware7]ntp-service unicast-server ?
  STRING<1-253>  Host name of the NTP server
  X.X.X.X        IP address of the NTP server

[Comware7]ntp-service unicast-server 10.0.100.251 ?
  authentication-keyid  Specify an authentication key ID
  priority              Specify the NTP peer as the first choice under the same
                        condition
  source                Specify a source interface
  version               Specify NTP version
  vpn-instance          Specify a VPN instance
  <cr>

[Comware7]ntp-service unicast-server 10.0.100.251

[Comware7]ntp-service enable ?
  <cr>

[Comware7]ntp-service enable


[Comware7]display ntp-service ?
  sessions  NTP connection
  status    NTP status and configuration information
  trace     Trace the time synchronization information

[Comware7]display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
******************************************************************************
[12345]10.0.100.251    216.218.192.202    2   255   64   18 3.1524 2.6092 4.0741
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1

[Comware7]display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 10.0.100.251
 Local mode: client
 Reference clock ID: 10.0.100.251
 Leap indicator: 00
 Clock jitter: 0.000153 s
 Stability: 0.000 pps
 Clock precision: 2^-17
 Root delay: 94.17725 ms
 Root dispersion: 11.99341 ms
 Reference time: d8be1d3e.190e4251  Thu, Mar 26 2015  0:53:02.097


[Comware7]clock ?
```

```
  protocol     Specify a time protocol
  summer-time  Configure daylight saving time
  timezone     Configure time zone

[Comware7]clock timezone ?
  STRING<1-32>  Name of time zone

[Comware7]clock timezone US-Central ?
  add    Add time zone offset
  minus  Minus time zone offset

[Comware7]clock timezone US-Central minus ?
  TIME  Time zone offset (hh:mm:ss)

[Comware7]clock timezone US-Central minus 06:00:00 ?
  <cr>

[Comware7]clock timezone US-Central minus 06:00:00


[Comware7]clock summer-time ?
  STRING<1-32>  Name of the daylight saving time

[Comware7]clock summer-time US-Central ?
  TIME  Time to start (HH:MM:SS)

[Comware7]clock summer-time US-Central 02:00:00 ?
  STRING<1-32>  Date to start (MM/DD)
  January       Start from January
  February      Start from February
  March         Start from March
  April         Start from April
  May           Start from May
  June          Start from June
  July          Start from July
  August        Start from August
  September     Start from September
  October       Start from October
  November      Start from November
  December      Start from December

[Comware7]clock summer-time US-Central 02:00:00 03/08 ?
  TIME  Time to end (hh:mm:ss)

[Comware7]clock summer-time US-Central 02:00:00 03/08 02:00:00 ?
  STRING<1-32>  Date to end (MM/DD)

[Comware7]clock summer-time US-Central 02:00:00 03/08 02:00:00 11/01 ?
  TIME  Time offset (hh:mm:ss)

[Comware7]clock summer-time US-Central 02:00:00 03/08 02:00:00 11/01 01:00:00 ?
  <cr>

[Comware7]clock summer-time US-Central 02:00:00 03/08 02:00:00 11/01 01:00:00


[Comware7]clock protocol ?
  none  Manually set the system time at the CLI
  ntp   Use the Network Time Protocol (NTP)
  ptp   Use the Precision Time Protocol (PTP)

[Comware7]clock protocol ntp ?
  <cr>
```

```
[Comware7]clock protocol ntp


[Comware7]display clock
01:08:21 US-Central Thu 03/26/2015
Time Zone : US-Central minus 06:00:00
Summer Time : US-Central 02:00:00 03/08 02:00:00 11/01 01:00:00
```

Cisco

```
Cisco(config)#ntp ?
  access-group        Control NTP access
  allow               Allow processing of packets
  authenticate        Authenticate time sources
  authentication-key  Authentication key for trusted time sources
  broadcastdelay      Estimated round-trip delay
  clock-period        Length of hardware clock tick
  logging             Enable NTP message logging
  master              Act as NTP master clock
  max-associations    Set maximum number of associations
  maxdistance         Maximum Distance for synchronization
  passive             NTP passive mode
  peer                Configure NTP peer
  server              Configure NTP server
  source              Configure interface for source address
  trusted-key         Key numbers for trusted time sources

Cisco(config)#ntp server ?
  A.B.C.D     IP address of peer
  WORD        Hostname of peer
  X:X:X:X::X  IPv6 address of peer
  ip          Use IP for DNS resolution
  ipv6        Use IPv6 for DNS resolution

Cisco(config)#ntp server 10.0.100.251 ?
  burst    Send a burst when peer is reachable
  iburst   Send a burst when peer is unreachable
  key      Configure peer authentication key
  maxpoll  Maximum poll interval
  minpoll  Minimum poll interval
  prefer   Prefer this peer when possible
  source   Interface for source address
  version  Configure NTP version
  <cr>

Cisco(config)#ntp server 10.0.100.251


Cisco#show ntp ?
  associations  NTP associations
  status        NTP status

Cisco#show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~10.0.100.251    216.218.192.20   2     25     64   177  2.322   2.130 64.390
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

Cisco#show ntp status
Clock is synchronized, stratum 3, reference is 10.0.100.251
nominal freq is 119.2092 Hz, actual freq is 119.2092 Hz, precision is 2**17
reference time is D8A9E976.CDEA704C (22:06:46.804 UTC Tue Mar 10 2015)
clock offset is 2.1303 msec, root delay is 102.49 msec
```

```
root dispersion is 447.09 msec, peer dispersion is 64.39 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000007 s/s
system poll interval is 64, last update was 178 sec ago.


Cisco(config)#clock ?
  initialize   Initialize system clock on restart
  save         backup of clock with NVRAM
  summer-time  Configure summer (daylight savings) time
  timezone     Configure time zone

Cisco(config)#clock timezone ?
  WORD  name of time zone

Cisco(config)#clock timezone US-Central ?
  <-23 - 23>  Hours offset from UTC

Cisco(config)#clock timezone US-Central -6 ?
  <0-59>  Minutes offset from UTC
  <cr>

Cisco(config)#clock timezone US-Central -6
%Time zone name is limited to 7 characters

Cisco(config)#clock timezone US-Cent -6


Cisco(config)#clock summer-time ?
  WORD  name of time zone in summer

Cisco(config)#clock summer-time US-Cent ?
  date       Configure absolute summer time
  recurring  Configure recurring summer time

Cisco(config)#clock summer-time US-Cent date ?
  <1-31>  Date to start
  MONTH   Month to start

Cisco(config)#clock summer-time US-Cent date mar ?
  <1-31>  Date to start

Cisco(config)#clock summer-time US-Cent date mar 8 ?
  <1993-2035>  Year to start

Cisco(config)#clock summer-time US-Cent date mar 8 2015 ?
  hh:mm  Time to start (hh:mm)

Cisco(config)#clock summer-time US-Cent date mar 8 2015 02:00 ?
  <1-31>  Date to end
  MONTH   Month to end

Cisco(config)#clock summer-time US-Cent date mar 8 2015 02:00 nov ?
  <1-31>  Date to end

Cisco(config)#clock summer-time US-Cent date mar 8 2015 02:00 nov 1 ?
  <1993-2035>  Year to end

Cisco(config)#clock summer-time US-Cent date mar 8 2015 02:00 nov 1 2015 ?
  hh:mm  Time to end (hh:mm)

Cisco(config)#clock summer-time US-Cent date mar 8 2015 02:00 nov 1 2015 02:00 ?
  <1-1440>  Offset to add in minutes
  <cr>
```

```
Cisco(config)#clock summer-time US-Cent date mar 8 2015 02:00 nov 1 2015 02:00 60 ?
  <cr>

Cisco(config)#clock summer-time US-Cent date mar 8 2015 02:00 nov 1 2015 02:00 60


Cisco#show clock
17:16:15.928 US-Cent Tue Mar 10 2015


Cisco#show clock detail
17:16:45.950 US-Cent Tue Mar 10 2015
Time source is NTP
Summer time starts 02:00:00 US-Cent Sun Mar 8 2015
Summer time ends 02:00:00 US-Cent Sun Nov 1 2015
```

b) SNTP

ArubaOS-Switch	Comware5	Cisco
ArubaOS-Switch(config)# sntp server priority 1 10.0.100.251	not supported	not supported on newer Cisco switches
ArubaOS-Switch(config)# sntp unicast		
ArubaOS-Switch(config)# sntp 60		
ArubaOS-Switch(config)# timesync sntp		
ArubaOS-Switch# show sntp authentication		
ArubaOS-Switch# show sntp statistics		
ArubaOS-Switch(config)# clock timezone us central		
ArubaOS-Switch(config)# clock summer-time		
ArubaOS-Switch(config)# time daylight-time-rule continental-us-and-canada		
ArubaOS-Switch# show time		
	Comware7	
	[Comware7]sntp enable	
	[Comware7]sntp unicast-server 10.0.100.251	
	[Comware7]clock timezone US-Central minus 06:00:00	
	[Comware7]clock summer-time US-Central 02:00:00 03/08 02:00:00 11/01 01:00:00	
	[Comware7]display clock	

ArubaOS-Switch

```
ArubaOS-Switch(config)# sntp ?
 authentication        Configure SNTP authentication
 broadcast             Operate in broadcast mode
 dhcp                  Operate in DHCP mode
 <30-720>              The number of seconds between updates of the system clock using
                       SNTP
 server                Configure a SNTP server to poll for time synchronization
 unicast               Operate in unicast mode
 <cr>

ArubaOS-Switch(config)# sntp server ?
 priority              Set the server priority

ArubaOS-Switch(config)# sntp server priority ?
 <1-3>                 Enter a number.
```

```
ArubaOS-Switch(config)# sntp server priority 1 ?
 IP-ADDR                The IPv4 address of the server
 IPV6-ADDR              The IPv6 address of the server

ArubaOS-Switch(config)# sntp server priority 1 10.0.100.251 ?
 oobm                   Use OOBM interface to connect to server
 <1-7>                  The SNTP version of the server
 <cr>

ArubaOS-Switch(config)# sntp server priority 1 10.0.100.251

ArubaOS-Switch(config)# sntp unicast

ArubaOS-Switch(config)# sntp 60

ArubaOS-Switch(config)# timesync sntp


ArubaOS-Switch# show sntp ?
 authentication         Show configured SNTP authentication information.
 statistics             Show SNTP protocol statistics.
 <cr>

ArubaOS-Switch# show sntp authentication ?
 <cr>

ArubaOS-Switch# show sntp authentication

  SNTP Authentication Information

  SNTP Authentication : Disabled

ArubaOS-Switch# show sntp statistics ?
 <cr>

ArubaOS-Switch# show sntp statistics

SNTP Statistics

  Received Packets  : 2
  Sent Packets      : 2
  Dropped Packets   : 0

  SNTP Server Address                              Auth Failed Pkts
  ---------------------------------------          ----------------
  10.0.100.251                                         0

ArubaOS-Switch# show sntp

 SNTP Configuration

  SNTP Authentication : Disabled
  Time Sync Mode: Sntp
  SNTP Mode : Unicast
  Poll Interval (sec) [720] : 60
  Source IP Selection: Outgoing Interface

  Priority SNTP Server Address                       Version Key-id
  -------- ---------------------------------------  ------- ----------
  1        10.0.100.251                              3       0


ArubaOS-Switch(config)# clock ?
```

```
 datetime               Specify the time and date
 set                    Set current time and/or date.
 summer-time            Enable/disable daylight-saving time changes.
 timezone               Set the number of hours your location is to the West(-) or East(+)
                        of GMT.
 <cr>

ArubaOS-Switch(config)# clock timezone ?
 gmt                    Number of hours your timezone is to the West(-) or East(+) of GMT.
 us                     Timezone for US locations.

ArubaOS-Switch(config)# clock timezone us
 alaska
 aleutian
 arizona
 central
 east_indiana
 eastern
 hawaii
 michigan
 mountain
 pacific
 samoa

ArubaOS-Switch(config)# clock timezone us central
 <cr>

ArubaOS-Switch(config)# clock summer-time
 <cr>


ArubaOS-Switch(config)# time ?
 begin-date             The begin date of daylight savings time
 MM/DD[/[YY]YY]         New date
 daylight-time-rule     The daylight savings time rule for your location
 end-date               The end date of daylight savings time
 HH:MM[:SS]             New time
 timezone               The number of minutes your location is West(-) or East(+) of GMT
 <cr>

ArubaOS-Switch(config)# time daylight-time-rule ?
 none
 alaska
 continental-us-and-canada
 middle-europe-and-portugal
 southern-hemisphere
 western-europe
 user-defined

ArubaOS-Switch(config)# time daylight-time-rule continental-us-and-canada ?
 begin-date             The begin date of daylight savings time
 MM/DD[/[YY]YY]         New date
 end-date               The end date of daylight savings time
 HH:MM[:SS]             New time
 timezone               The number of minutes your location is West(-) or East(+) of GMT
 <cr>

ArubaOS-Switch(config)# time daylight-time-rule continental-us-and-canada


ArubaOS-Switch# show time
Tue Mar 10 15:50:11 2015
```

Comware5

not supported

Comware7

```
[Comware7]sntp enable
[Comware7]sntp unicast-server 10.0.100.251 ?
  authentication-keyid  Specify an authentication key ID
  source                Specify a source interface
  version               Specify SNTP version
  vpn-instance          Specify a VPN instance
  <cr>

[Comware7]sntp unicast-server 10.0.100.251


[Comware7]display sntp ?
  ipv6      IPv6 protocol
  sessions  Session information

[Comware7]display sntp sessions ?
  >     Redirect it to a file
  >>    Redirect it to a file in append mode
  |     Matching output
  <cr>

[Comware7]display sntp sessions
SNTP server     Stratum   Version    Last receive time
10.0.100.251    2         4          Thu, Mar 26 2015  1:16:58.143


[Comware7]clock ?
  protocol     Specify a time protocol
  summer-time  Configure daylight saving time
  timezone     Configure time zone

[Comware7]clock timezone ?
  STRING<1-32>  Name of time zone

[Comware7]clock timezone US-Central ?
  add    Add time zone offset
  minus  Minus time zone offset

[Comware7]clock timezone US-Central minus ?
  TIME  Time zone offset (hh:mm:ss)

[Comware7]clock timezone US-Central minus 06:00:00 ?
  <cr>

[Comware7]clock timezone US-Central minus 06:00:00


[Comware7]clock summer-time ?
  STRING<1-32>  Name of the daylight saving time

[Comware7]clock summer-time US-Central ?
  TIME  Time to start (HH:MM:SS)

[Comware7]clock summer-time US-Central 02:00:00 ?
  STRING<1-32>  Date to start (MM/DD)
  January       Start from January
  February      Start from February
```

```
  March          Start from March
  April          Start from April
  May            Start from May
  June           Start from June
  July           Start from July
  August         Start from August
  September      Start from September
  October        Start from October
  November       Start from November
  December       Start from December

[Comware7]clock summer-time US-Central 02:00:00 03/08 ?
  TIME  Time to end (hh:mm:ss)

[Comware7]clock summer-time US-Central 02:00:00 03/08 02:00:00 ?
  STRING<1-32>  Date to end (MM/DD)

[Comware7]clock summer-time US-Central 02:00:00 03/08 02:00:00 11/01 ?
  TIME  Time offset (hh:mm:ss)

[Comware7]clock summer-time US-Central 02:00:00 03/08 02:00:00 11/01 01:00:00 ?
  <cr>

[Comware7]clock summer-time US-Central 02:00:00 03/08 02:00:00 11/01 01:00:00


[Comware7]display clock
01:29:21 US-Central Thu 03/26/2015
Time Zone : US-Central minus 06:00:00
Summer Time : US-Central 02:00:00 03/08 02:00:00 11/01 01:00:00
```

Cisco

not supported on newer Cisco switches

Chapter 7 SNMP

This chapter compares the commands you use to configure Simple Network Management Protocol (SNMP).

- On ArubaOS-Switch, SNMP v1/v2c is enabled by default.
- On Comware, SNMP v3 is the configured version, disabled by default.
- On Cisco, SNMP is disabled by default.

SNMP is an Internet standard protocol that enables a Network Management System (NMS) to access and operate the devices on a network, regardless of their vendors, physical characteristics, and interconnect technologies.

SNMP enables network administrators to read and set the variables on managed devices for state monitoring, troubleshooting, statistics collection, and other management purposes.

The following elements comprise the SNMP framework:

- SNMP manager—Runs on an NMS, monitoring and managing the SNMP-capable devices in the network
- SNMP agent—Runs on a managed device, receiving and handling requests from the NMS, and sending traps to the NMS when some events, such as an interface state change, occur
- Management information base (MIB)—Specifies the variables (for example, interface status and CPU usage) maintained by the SNMP agent for the SNMP manager to read and set

A MIB stores variables called "nodes" or "objects" in a tree hierarchy and identifies each node with a unique oject identifier (OID). An OID is a string of numbers that describes the path from the root node to a leaf node. There are both “public” and “private” or manufacturer/device-specific MIB definitions.

HP and Cisco support SNMPv1, SNMPv2c, and SNMPv3. An NMS and an SNMP agent must use the same SNMP version to communicate with each other.

- SNMPv1 uses community names for authentication. To access an SNMP agent, an NMS must use the same community name as the SNMP agent. If the community name the NMS uses is different from the agent’s, the NMS cannot establish an SNMP session to access the agent or receive traps from the agent.
- SNMPv2c uses community names for authentication. SNMPv2c is compatible with SNMPv1, but supports more operation modes, data types, and error codes.
- SNMPv3 uses a user-based security model (USM) to secure SNMP communication. You can configure authentication and privacy mechanisms to authenticate and encrypt SNMP packets for integrity, authenticity, and confidentiality.

a) SNMP Version 1 and Version 2c

ArubaOS-Switch	Comware	Cisco
[snmp v1/v2c is default version]		
ArubaOS-Switch(config)# snmp-server host 10.0.111.210 community private trap-level all	[Comware]snmp-agent target-host trap address udp-domain 10.0.111.210 udp-port 161 pa rams securityname private	Cisco(config)#snmp-server host 10.0.111.210 version 2c private
ArubaOS-Switch(config)# snmp-server community public operator restricted	[Comware]snmp-agent community read public	Cisco(config)#snmp-server community public ro
ArubaOS-Switch(config)# snmp-server community private manager unrestricted	[Comware]snmp-agent community write private	Cisco(config)#snmp-server community private rw
ArubaOS-Switch(config)# snmp-server location Lab	[Comware]snmp-agent sys-info location Lab	Cisco(config)#snmp-server location Lab
ArubaOS-Switch(config)# snmp-server contact Lab_Engr	[Comware]snmp-agent sys-info contact Lab_Engr	Cisco(config)#snmp-server contact Lab_Engr
	[Comware]snmp-agent sys-info version v1 v2c [Comware]undo snmp-agent sys-info version v3	
ArubaOS-Switch(config)# snmp-server enable	[Comware]snmp-agent trap enable [Comware]snmp-agent	Cisco(config)#snmp-server enable traps
ArubaOS-Switch# show snmp-server	[Comware]display snmp-agent sys-info [Comware]display snmp-agent community	Cisco#show snmp Cisco#show snmp host

ArubaOS-Switch

[snmp v1/v2c is default version]

```
ArubaOS-Switch(config)# snmp-server ?
 community              Add/delete SNMP community.
 contact                Name of the switch administrator.
 enable                 Enable/Disable SNMPv1/v2.
 engine-id              Set the SNMPv3 Engine ID.
 host                   Define SNMP traps and their receivers.
 listen                 Usage: snmp-server listen [oobm|data|both]Specify in which mode
                        SNMP Server should listen in.
 location               Description of the switch location.
 mib                    Enable/Disable SNMP support for the hpSwitchAuthentication MIB.
 response-source        Specify the source ip-address policy for the response pdu.
 trap-source            Specify the source ip-address policy for the trap pdu.

ArubaOS-Switch(config)# snmp-server host ?
 IP-ADDR                IP address of SNMP notification host.
 IPV6-ADDR              IPv6 address of SNMP notification host.

ArubaOS-Switch(config)# snmp-server host 10.0.111.210 ?
 community              Name of the SNMP community (up to 32 characters).
 informs                Specify if informs will be sent, rather than notifications.
 oobm                   Use OOBM interface to connect to server
```

```
 trap-level            Specify the trap level [none|debug|all|not-info|critical].

ArubaOS-Switch(config)# snmp-server host 10.0.111.210 community ?
 COMMUNITY-NAME-STR    Name of the SNMP community (up to 32 characters).

ArubaOS-Switch(config)# snmp-server host 10.0.111.210 community private ?
 informs               Specify if informs will be sent, rather than notifications.
 oobm                  Use OOBM interface to connect to server
 trap-level            Specify the trap level [none|debug|all|not-info|critical].
 <cr>

ArubaOS-Switch(config)# snmp-server host 10.0.111.210 community private trap-level ?
 none                  Send no log messages.
 debug                 Send debug traps (for Internal use).
 all                   Send all log messages
 not-info              Send all but informational-only messages.
 critical              Send critical-level log messages.

ArubaOS-Switch(config)# snmp-server host 10.0.111.210 community private trap-level all ?
 informs               Specify if informs will be sent, rather than notifications.
 oobm                  Use OOBM interface to connect to server
 <cr>
ArubaOS-Switch(config)# snmp-server host 10.0.111.210 community private trap-level all


ArubaOS-Switch(config)# snmp-server community ?
 ASCII-STR             Enter an ASCII string.

ArubaOS-Switch(config)# snmp-server community public ?
 operator              The community can access only limited set of MIB objects which
                       includes monitoring objects and a limited set of configuration
                       objects.
 manager               The community can access all MIB objects.
 restricted            MIB variables cannot be set, only read.
 unrestricted          Any MIB variable that has read/write access can be set.
 <cr>

ArubaOS-Switch(config)# snmp-server community public operator ?
 restricted            MIB variables cannot be set, only read.
 unrestricted          Any MIB variable that has read/write access can be set.
 <cr>

ArubaOS-Switch(config)# snmp-server community public operator restricted ?
 <cr>

ArubaOS-Switch(config)# snmp-server community public operator restricted


ArubaOS-Switch(config)# snmp-server community private ?
 operator              The community can access only limited set of MIB objects which
                       includes monitoring objects and a limited set of configuration
                       objects.
 manager               The community can access all MIB objects.
 restricted            MIB variables cannot be set, only read.
 unrestricted          Any MIB variable that has read/write access can be set.
 <cr>

ArubaOS-Switch(config)# snmp-server community private manager ?
 restricted            MIB variables cannot be set, only read.
 unrestricted          Any MIB variable that has read/write access can be set.
 <cr>

ArubaOS-Switch(config)# snmp-server community private manager unrestricted ?
```

```
 <cr>

ArubaOS-Switch(config)# snmp-server community private manager unrestricted


ArubaOS-Switch(config)# snmp-server location
 ASCII-STR             Enter an ASCII string.

ArubaOS-Switch(config)# snmp-server location Lab

ArubaOS-Switch(config)# snmp-server contact
 ASCII-STR             Enter an ASCII string.

ArubaOS-Switch(config)# snmp-server contact Lab_Engr

ArubaOS-Switch(config)# snmp-server enable
 traps                 Enable/disable event traps to be sent by the switch.
 <cr>

ArubaOS-Switch(config)# snmp-server enable traps
 arp-protect           Traps for Dynamic ARP Protection.
 auth-server-fail      Traps reporting authentication server unreachable.
 dhcp-server           Traps for DHCP-Server
 dhcp-snooping         Traps for DHCP-Snooping.
 dhcpv6-snooping       Set the traps for DHCPv6 snooping.
 dyn-ip-lockdown       Traps for Dynamic Ip Lockdown
 dyn-ipv6-lockdown     Traps for Dynamic IPv6 Lockdown.
 link-change           Traps for link-up and link-down.
 login-failure-mgr     Traps for management interface login failure.
 mac-count-notify      Traps for MAC addresses learned on the specified ports exceeds the
                       threshold.
 mac-notify            Traps for (learned/removed) MAC address table changes.
 password-change-mgr   Traps for management interface password change.
 port-security         Traps for port access authentication failure.
 running-config-change Traps for running config change.
 snmp-authentication   Select RFC-1157 (standard) or HP-ICF-SNMP (extended) traps.
 startup-config-change Traps for changes to the startup config.

ArubaOS-Switch(config)# snmp-server enable


ArubaOS-Switch# show snmp-server


 SNMP Communities

  Community Name                   MIB View Write Access
  -------------------------------- -------- ------------
  public                           Operator Restricted
  private                          Manager  Unrestricted

 Trap Receivers

  Link-Change Traps Enabled on Ports [All] : All

  Traps Category                          Current Status
  _____________________________________  __________________
  SNMP Authentication                   : Extended
  Password change                       : Enabled
  Login failures                        : Enabled
  Port-Security                         : Enabled
  Authorization Server Contact          : Enabled
  DHCP-Snooping                         : Enabled
```

```
  DHCPv6-Snooping Out of Resource       : Enabled
  DHCPv6-Snooping Errant Replies        : Enabled
  Dynamic ARP Protection                : Enabled
  Dynamic IP Lockdown                   : Enabled
  Dynamic IPv6 Lockdown Out of Resource : Enabled
  Dynamic IPv6 Lockdown Violations      : Enabled
  Startup Config change                 : Disabled
  Running Config Change                 : Disabled
  MAC address table changes             : Disabled
  MAC Address Count                     : Disabled
  DHCP-Server                           : Enabled

  Address                 Community              Events   Type   Retry   Timeout
  ----------------------- ---------------------- -------- ------ ------- -------
  10.0.111.210            private                All      trap   3       15


 Excluded MIBs


 Snmp Response Pdu Source-IP Information

  Selection Policy   : rfc1517

 Trap Pdu Source-IP Information

  Selection Policy   : configuredIP
  IP Address         : 10.0.111.21
```

Comware5

```
[Comware5]snmp-agent ?
  calculate-password  Calculate the secret key of the plain password
  community           Set a community for the access of SNMPv1&SNMPv2c
  group               Set a SNMP group based on USM
  ifmib               IF-MIB commands
  local-engineid      Set the engineID of local SNMP entity
  log                 Set the log function
  mib-view            Set SNMP MIB view information
  packet              Set SNMP packet's parameters
  sys-info            Set system information of the node
  target-host         Set the target hosts to receive SNMP notification/traps
  trap                Set the parameters of SNMP trap/notification
  usm-user            Set a new user for access to SNMP entity
  <cr>

[Comware5]snmp-agent target-host ?
  trap  Specify trap host target

[Comware5]snmp-agent target-host trap ?
  address  Specify the transport addresses to be used in the generation of SNMP
           messages

[Comware5]snmp-agent target-host trap address ?
  udp-domain  Specify transport domain over UDP for the target host

[Comware5]snmp-agent target-host trap address udp-domain ?
  STRING<1-255>  IP address or hostname of target host
  ipv6           Specify an ipv6 address as the target host address

[Comware5]snmp-agent target-host trap address udp-domain 10.0.111.210 ?
  dscp          Differentiated Services Code Point
  params        Specify SNMP target information to be used in the generation of
                SNMP messages
```

```
  udp-port      Set port to receive traps/notifications for this target host
  vpn-instance  Specify VPN instance

[Comware5]snmp-agent target-host trap address udp-domain 10.0.111.210 udp-port ?
  INTEGER<0-65535>  The port number of target host

[Comware5]snmp-agent target-host trap address udp-domain 10.0.111.210 udp-port 161 ?
  dscp          Differentiated Services Codepoint (DSCP)
  params        Specify SNMP target information to be used in the generation of
                SNMP messages
  vpn-instance  Specify VPN instance

[Comware5]snmp-agent target-host trap address udp-domain 10.0.111.210 udp-port 161 pa
rams ?
  securityname  Specify the name for the principal on whose behalf SNMP
                messages will be generated

[Comware5]snmp-agent target-host trap address udp-domain 10.0.111.210 udp-port 161 pa
rams securityname ?
  STRING<1-32>  Specify the character string of security name

[Comware5]snmp-agent target-host trap address udp-domain 10.0.111.210 udp-port 161 pa
rams securityname private ?
  v1    Specify security model of SNMPv1 to generate SNMP messages
  v2c   Specify security model of SNMPv2c to generate SNMP messages
  v3    Specify security model of SNMPv3 to generate SNMP messages
  <cr>

[Comware5]snmp-agent target-host trap address udp-domain 10.0.111.210 udp-port 161 pa
rams securityname private

[Comware5]snmp-agent community ?
  read   Read-only access for this community string
  write  Read-write access for this community string

[Comware5]snmp-agent community read ?
  STRING<1-32>  SNMP community string

[Comware5]snmp-agent community read public ?
  acl       Set access control list for this community
  mib-view  MIB view for which this community is restricted
  <cr>

[Comware5]snmp-agent community read public

[Comware5]snmp-agent community write ?
  STRING<1-32>  SNMP community string

[Comware5]snmp-agent community write private ?
  acl       Set access control list for this community
  mib-view  MIB view for which this community is restricted
  <cr>

[Comware5]snmp-agent community write private

[Comware5]snmp-agent sys-info ?
  contact   Set the contact information for system maintenance
  location  Set the physical position information of this node
  version   Enable the SNMP protocol version

[Comware5]snmp-agent sys-info location ?
  TEXT  The physical location of this node<1-255>
```

```
[Comware5]snmp-agent sys-info location Lab

[Comware5]snmp-agent sys-info contact ?
  TEXT  Contact person information for this node<1-255>

[Comware5]snmp-agent sys-info contact Lab_Engr

[Comware5]snmp-agent sys-info version ?
  all  Enable the device to support SNMPv1, SNMPv2c and SNMPv3
  v1   Enable the device to support SNMPv1
  v2c  Enable the device to support SNMPv2c
  v3   Enable the device to support SNMPv3

[Comware5]snmp-agent sys-info version v1 ?
  v2c   Enable the device to support SNMPv2c
  v3    Enable the device to support SNMPv3
  <cr>

[Comware5]snmp-agent sys-info version v1 v2c ?
  v3    Enable the device to support SNMPv3
  <cr>

[Comware5]snmp-agent sys-info version v1 v2c

[Comware5]undo snmp-agent sys-info version v3
  (Note, SNMP v3 is configured but not enabled, so if only v1 & v2c required, undo v3)

[Comware5]snmp-agent trap ?
  enable      SNMP trap/notification enable commands group
  if-mib      Set trap types in IF-MIB
  life        Set the trap aging time
  queue-size  Length of each TRAP message queue
  source      Set the source address of traps

[Comware5]snmp-agent trap enable ?
  arp            Enable ARP traps
  bfd            Enable BFD traps
  bgp            Enable BGP trap
  configuration  Enable the configuration management traps
  default-route  Enable default route traps
  flash          Enable Flash traps
  ospf           Enable OSPF traps
  pim            Enable PIM traps
  standard       Enable the standard SNMP traps
  system         Enable SysMib traps
  vrrp           Enable VRRP traps
  <cr>

[Comware5]snmp-agent trap enable

[Comware5]snmp-agent


[Comware5]display snmp-agent sys-info
   The contact person for this managed node:
           LabEngr

   The physical location of this node:
           Lab

   SNMP version running in the system:
           SNMPv1 SNMPv2c
```

```
[Comware5]display snmp-agent community
   Community name: public
       Group name: public
       Storage-type: nonVolatile

   Community name: private
       Group name: private
       Storage-type: nonvolatile
```

Comware7

```
[Comware7]snmp-agent ?
  calculate-password  Convert a plain text key to an encrypted key
  community           Set a community for the access of SNMPv1 and SNMPv2c
  community-map       Configure an SNMP community to map
  context             Configure an SNMP context
  group               Set an SNMP group based on USM
  inform              Set the parameters of SNMP inform
  local-engineid      Set the engine ID for the local SNMP agent
  log                 Enable the logging function
  mib-view            Set an SNMP MIB view
  packet              Set the SNMP packet size
  port                Specify an SNMP port
  remote              Configure a remote engine
  sys-info            Set system information of the agent
  target-host         Set a target host to receive SNMP notifications
  trap                Set the parameters of SNMP notifications
  usm-user            Add an SNMP user to an SNMP group
  <cr>

[Comware7]snmp-agent target-host ?
  inform  Set a target host to receive SNMP informs
  trap    Set a target host to receive SNMP traps

[Comware7]snmp-agent target-host trap ?
  address  Specify the transport address of the target host

[Comware7]snmp-agent target-host trap address ?
  udp-domain  Use UDP to transport SNMP information

[Comware7]snmp-agent target-host trap address udp-domain ?
  STRING<1-253>  IP address or hostname of the target host
  ipv6           IPv6 address of the target host

[Comware7]snmp-agent target-host trap address udp-domain 10.0.111.210 ?
  params        Specify SNMP information to be used in the generation of SNMP
                notifications
  udp-port      Set port to receive notifications for the target host
  vpn-instance  Specify VPN instance

[Comware7]snmp-agent target-host trap address udp-domain 10.0.111.210 udp-port ?
  INTEGER<0-65535>  Port number

[Comware7]snmp-agent target-host trap address udp-domain 10.0.111.210 udp-port 161 ?
  params        Specify SNMP information to be used in the generation of SNMP
                notifications
  vpn-instance  Specify VPN instance

[Comware7]snmp-agent target-host trap address udp-domain 10.0.111.210 udp-port 161 params ?
  securityname  Specify the security name for the principal on whose behalf SNMP
                notifications will be generated

[Comware7]snmp-agent target-host trap address udp-domain 10.0.111.210 udp-port 161 params
securityname ?
```

```
  STRING<1-32>  Security name

[Comware7]snmp-agent target-host trap address udp-domain 10.0.111.210 udp-port 161 params
securityname private ?
  v1    Set the security model to SNMPv1 for generating SNMP notifications
  v2c   Set the security model to SNMPv2 for generating SNMP notifications
  v3    Set the security model to SNMPv3 for generating SNMP notifications
  <cr>

[Comware7]snmp-agent target-host trap address udp-domain 10.0.111.210 udp-port 161 params
securityname private

[Comware7]snmp-agent community ?
  STRING<1-32>  Plaintext community name
  cipher        Specify a ciphertext community name
  read          Assign the community the read-only access to MIB objects
  simple        Specify a plaintext community name
  write         Assign the community the read and write access to MIB objects

[Comware7]snmp-agent community read ?
  STRING<1-32>  Plaintext community name
  cipher        Specify a ciphertext community name
  simple        Specify a plaintext community name

[Comware7]snmp-agent community read public ?
  acl       Set access control list for this user
  mib-view  Specify the MIB views available for the community
  <cr>

[Comware7]snmp-agent community read public

[Comware7]snmp-agent community write ?
  STRING<1-32>  Plaintext community name
  cipher        Specify a ciphertext community name
  simple        Specify a plaintext community name

[Comware7]snmp-agent community write private ?
  acl       Set access control list for this user
  mib-view  Specify the MIB views available for the community
  <cr>

[Comware7]snmp-agent community write private

[Comware7]snmp-agent sys-info ?
  contact   Specify the contact for system maintenance
  location  Set the location information of the agent
  version   Specify the SNMP version

[Comware7]snmp-agent sys-info location ?
  TEXT  Location information of the agent, 1 to 255 characters

[Comware7]snmp-agent sys-info location Lab

[Comware7]snmp-agent sys-info contact ?
  TEXT  Contact information, 1 to 255 characters

[Comware7]snmp-agent sys-info contact Lab_Engr

[Comware7]snmp-agent sys-info version ?
  all  Enable the agent to support SNMPv1, SNMPv2c and SNMPv3
  v1   Enable the agent to support SNMPv1
  v2c  Enable the agent to support SNMPv2c
  v3   Enable the agent to support SNMPv3
```

```
[Comware7]snmp-agent sys-info version v1 ?
  v2c   Enable the agent to support SNMPv2c
  v3    Enable the agent to support SNMPv3
  <cr>

[Comware7]snmp-agent sys-info version v1 v2c ?
  v3    Enable the agent to support SNMPv3
  <cr>

[Comware7]snmp-agent sys-info version v1 v2c

[Comware7]undo snmp-agent sys-info version v3
  (Note, SNMP v3 is configured but not enabled, so if only v1 & v2c required, undo v3)

[Comware7]snmp-agent trap ?
  enable               Enable SNMP notifications
  if-mib               Set the notification format in the IF-MIB
  life                 Set the notifications aging time
  log                  Enable logging of Notifications
  periodical-interval  Specify the interval for sending periodical notifications
  queue-size           Set the length of the notification queue
  source               Set the source IP address for notifications

[Comware7]snmp-agent trap enable ?
  arp            ARP module
  bgp            Enable BGP notifications
  configuration  Enable configuration management notifications
  ike            Enable SNMP notifications for IKE
  ipsec          Enable SNMP notifications for IPsec events
  isis           IS-IS module
  l3vpn          Enable L3VPN notifications
  ldp            Enable LDP notifications
  mac-address    Enable MAC address notification
  mpls           Enable MPLS notifications
  ospf           OSPF module
  ospfv3         OSPFv3 module
  radius         RADIUS module
  spbm           Enable SPBM notifications
  standard       Enable standard SNMP notification
  system         Enable system management notifications
  trill          Enable TRILL notifications
  vrrp           Enable VRRP notifications
  <cr>

[Comware7]snmp-agent trap enable

[Comware7]snmp-agent


[Comware7]display snmp-agent sys-info
  The contact information of the agent:
      Lab_Engr

  The location information of the agent:
      lab

  The SNMP version of the agent:
      SNMPv1 SNMPv2c

[Comware7]display snmp-agent community
   Community name: private
       Group name: private
```

```
        Storage-type: nonVolatile

    Community name: public
        Group name: public
        Storage-type: nonVolatile
```

Cisco

```
Cisco(config)#snmp-server ?
  cache              Enable SNMP cache
  chassis-id         String to uniquely identify this chassis
  community          Enable SNMP; set community string and access privs
  contact            Text for mib object sysContact
  context            Create/Delete a context apart from default
  enable             Enable SNMP Traps
  engineID           Configure a local or remote SNMPv3 engineID
  file-transfer      File transfer related commands
  group              Define a User Security Model group
  host               Specify hosts to receive SNMP notifications
  ifindex            Enable ifindex persistence
  inform             Configure SNMP Informs options
  ip                 IP ToS configuration for SNMP traffic
  location           Text for mib object sysLocation
  manager            Modify SNMP manager parameters
  packetsize         Largest SNMP packet size
  queue-length       Message queue length for each TRAP host
  source-interface   Assign an source interface
  spi                Configs for SNMP communication using SPI
  sysobjectid        sysObjectID
  system-shutdown    Enable use of the SNMP reload command
  tftp-server-list   Limit TFTP servers used via SNMP
  trap               SNMP trap options
  trap-source        Assign an interface for the source address of all traps
  trap-timeout       Set timeout for TRAP message retransmissions
  user               Define a user who can access the SNMP engine
  view               Define an SNMPv3 MIB view

Cisco(config)#snmp-server host ?
  WORD                                                    IP/IPV6 address of SNMP
                                                          notification host
  http://<Hostname or A.B.C.D>[:<port number>][/<uri>]  HTTP address of XML
                                                          notification host

Cisco(config)#snmp-server host 10.0.111.210 ?
  WORD     SNMPv1/v2c community string or SNMPv3 user name
  informs  Send Inform messages to this host
  traps    Send Trap messages to this host
  version  SNMP version to use for notification messages
  vrf      VPN Routing instance for this host

Cisco (config)#snmp-server host 10.0. 11.210 version ?
  1   Use SNMPv1
  2c  Use SNMPv2c
  3   Use SNMPv3

Cisco(config)#snmp-server host 10.0.111.210 version 2c ?
  WORD  SNMPv1/v2c community string or SNMPv3 user name

Cisco(config)#snmp-server host 10.0.111.210 version 2c private ?
  auth-framework    Allow SNMP CISCO-AUTH-FRAMEWORK-MIB traps
  bridge            Allow SNMP STP Bridge MIB traps
  call-home         Allow SNMP CISCO-CALLHOME-MIB traps
  cef               Allows cef traps
  cluster           Allow Cluster Member Status traps
```

```
  config             Allow SNMP config traps
  config-copy        Allow SNMP config-copy traps
  config-ctid        Allow SNMP config-ctid traps
  copy-config        Allow SNMP copy-config traps
  cpu                Allow cpu related traps
  dot1x              Allow dot1x traps
  eigrp              Allow SNMP EIGRP traps
  energywise         Allow SNMP energywise traps
  entity             Allow SNMP entity traps
  envmon             Allow environmental monitor traps
  errdisable         Allow errordisable notifications
  event-manager      Allow SNMP Embedded Event Manager traps
  flash              Allow SNMP FLASH traps
  flowmon            Allow SNMP flow monitor notifications
  fru-ctrl           Allow entity FRU control traps
  hsrp               Allow SNMP HSRP traps
  ipmulticast        Allow SNMP ipmulticast traps
  ipsla              Allow SNMP Host IP SLA traps
  license            Allow license traps
  mac-notification   Allow SNMP MAC Notification Traps
  ospf               Allow OSPF traps
  pim                Allow SNMP PIM traps
  port-security      Allow SNMP port-security traps
  power-ethernet     Allow SNMP power ethernet traps
  snmp               Allow SNMP-type notifications
  stackwise          Allow SNMP stackwise traps
  storm-control      Allow SNMP storm-control traps
  stpx               Allow SNMP STPX MIB traps
  syslog             Allow SNMP syslog traps
  tty                Allow TCP connection traps
  udp-port           The notification host's UDP port number (default port 162)
  vlan-membership    Allow SNMP VLAN membership traps
  vlancreate         Allow SNMP VLAN created traps
  vlandelete         Allow SNMP VLAN deleted traps
  vstack             Allow SNMP Smart Install traps
  vtp                Allow SNMP VTP traps
  <cr>

Cisco(config)#snmp-server host 10.0.111.210 version 2c private


Cisco(config)#snmp-server community ?
  WORD  SNMP community string

Cisco(config)#snmp-server community public ?
  <1-99>       Std IP accesslist allowing access with this community string
  <1300-1999>  Expanded IP accesslist allowing access with this community
               string
  WORD         Access-list name
  ro           Read-only access with this community string
  rw           Read-write access with this community string
  view         Restrict this community to a named MIB view
  <cr>

Cisco(config)#snmp-server community public ro ?
  <1-99>       Std IP accesslist allowing access with this community string
  <1300-1999>  Expanded IP accesslist allowing access with this community
               string
  WORD         Access-list name
  ipv6         Specify IPv6 Named Access-List
  <cr>

Cisco(config)#snmp-server community public ro
```

```
Cisco(config)#snmp-server community private ?
  <1-99>       Std IP accesslist allowing access with this community string
  <1300-1999>  Expanded IP accesslist allowing access with this community
               string
  WORD         Access-list name
  ro           Read-only access with this community string
  rw           Read-write access with this community string
  view         Restrict this community to a named MIB view
  <cr>

Cisco(config)#snmp-server community private rw ?
  <1-99>       Std IP accesslist allowing access with this community string
  <1300-1999>  Expanded IP accesslist allowing access with this community
               string
  WORD         Access-list name
  ipv6         Specify IPv6 Named Access-List
  <cr>

Cisco(config)#snmp-server community private rw


Cisco(config)#snmp-server location ?
  LINE  The physical location of this node

Cisco(config)#snmp-server location Lab

Cisco(config)#snmp-server contact ?
  LINE  identification of the contact person for this managed node

Cisco(config)#snmp-server contact Lab_Engr

Cisco(config)#snmp-server enable ?
  traps  Enable SNMP Traps

Cisco(config)#snmp-server enable traps ?
  auth-framework    Enable SNMP CISCO-AUTH-FRAMEWORK-MIB traps
  bridge            Enable SNMP STP Bridge MIB traps
  call-home         Enable SNMP CISCO-CALLHOME-MIB traps
  cef               Enable SNMP CEF traps
  cluster           Enable Cluster traps
  config            Enable SNMP config traps
  config-copy       Enable SNMP config-copy traps
  config-ctid       Enable SNMP config-ctid traps
  copy-config       Enable SNMP config-copy traps
  cpu               Allow cpu related traps
  dot1x             Enable SNMP dot1x traps
  eigrp             Enable SNMP EIGRP traps
  energywise        Enable SNMP ENERGYWISE traps
  entity            Enable SNMP entity traps
  envmon            Enable SNMP environmental monitor traps
  errdisable        Enable SNMP errdisable notifications
  event-manager     Enable SNMP Embedded Event Manager traps
  flash             Enable SNMP FLASH notifications
  flowmon           Enabel SNMP flowmon notifications
  fru-ctrl          Enable SNMP entity FRU control traps
  hsrp              Enable SNMP HSRP traps
  ipmulticast       Enable SNMP ipmulticast traps
  ipsla             Enable SNMP IP SLA traps
  license           Enable license traps
  mac-notification  Enable SNMP MAC Notification traps
  ospf              Enable OSPF traps
  pim               Enable SNMP PIM traps
```

```
  port-security     Enable SNMP port security traps
  power-ethernet    Enable SNMP power ethernet traps
  snmp              Enable SNMP traps
  stackwise         Enable SNMP stackwise traps
  storm-control     Enable SNMP storm-control trap parameters
  stpx              Enable SNMP STPX MIB traps
  syslog            Enable SNMP syslog traps
  transceiver       Enable SNMP transceiver traps
  tty               Enable TCP connection traps
  vlan-membership   Enable SNMP VLAN membership traps
  vlancreate        Enable SNMP VLAN created traps
  vlandelete        Enable SNMP VLAN deleted traps
  vstack            Enable SNMP Smart Install traps
  vtp               Enable SNMP VTP traps
  <cr>

Cisco(config)#snmp-server enable traps


Cisco#show snmp
Chassis: FDO1231V0US
Contact: Lab_Engr
Location: Lab
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
SNMP global trap: enabled

SNMP logging: enabled
    Logging to 10.0.111.210.162, 0/10, 0 sent, 0 dropped.
SNMP agent enabled

Cisco#show snmp host
Notification host: 10.0.111.210  udp-port: 162   type: trap
user: private   security model: v2c
```

b) SNMP Version 3

ArubaOS-Switch	Comware	Cisco
	[snmp v3 is default version]	
ArubaOS-Switch(config)# snmpv3 enable		
	[Comware]snmp-agent group v3 <name> privacy	Cisco(config)#snmp-server group <name> v3 priv
ArubaOS-Switch(config)# snmpv3 user test auth md5 password priv des password		
	[Comware]snmp-agent usm-user v3 test managerpriv authentication-mode md5 password privacy-mode des password	Cisco(config)#snmp-server user test managerpriv v3 auth md5 password priv des password
ArubaOS-Switch(config)# snmpv3 group managerpriv user test sec-model ver3		
ArubaOS-Switch(config)# snmpv3 targetaddress NMS params all 10.0.111.210	[Comware]snmp-agent target-host trap address udp-domain 10.0.111.210 params securityname test v3 privacy	Cisco(config)#snmp-server host 10.0.111.210 version 3 priv test
ArubaOS-Switch(config)# snmp-server location Lab	[Comware]snmp-agent sys-info location Lab	Cisco(config)#snmp-server location Lab
ArubaOS-Switch(config)# snmp-server contact Lab_Engr	[Comware]snmp-agent sys-info contact Lab_Engr	Cisco(config)#snmp-server contact Lab_Engr
ArubaOS-Switch# show snmpv3 enable ArubaOS-Switch# show snmpv3 targetaddress	[Comware]display snmp-agent sys-info	Cisco#show snmp host
ArubaOS-Switch# show snmpv3 user	[Comware]display snmp-agent usm-user	Cisco#show snmp user
ArubaOS-Switch# show snmpv3 group	[Comware]display snmp-agent group	Cisco#show snmp group

ArubaOS-Switch

```
ArubaOS-Switch(config)# snmpv3 ?
 community              Configure SNMPv3 Community entry.
 enable                 Enable SNMPv3.
 group                  Configure SNMPv3 User to Group entry.
 notify                 Configure SNMPv3 Notification entry.
 only                   Accept only SNMP v3 messages.
 params                 Configure SNMPv3 Target Parameter entry.
 restricted-access      Configure SNMPv1 and SNMPv2c access properties.
 targetaddress          Configure SNMPv3 Target Address entry.
 user                   Configure SNMPv3 User entry.

ArubaOS-Switch(config)# snmpv3 enable
SNMPv3 Initialization process.
Creating user 'initial'
Authentication Protocol: MD5
Enter authentication password: ********
Privacy protocol is DES
Enter privacy password: ********
```

```
User 'initial' is created
Would you like to create a user that uses SHA? [y/n] y
Enter user name: initial
Authentication Protocol: SHA
Enter authentication password: ********
Privacy protocol is DES
Enter privacy password: ********

User creation is done.  SNMPv3 is now functional.
Would you like to restrict SNMPv1 and SNMPv2c messages to have read only
access (you can set this later by the command 'snmp restrict-access')? [y/n] y


ArubaOS-Switch(config)# snmpv3 user ?
 USERNAME-STR          Set authentication parameters.

ArubaOS-Switch(config)# snmpv3 user test ?
 auth                  Set authentication parameters. If in enhanced secure-mode, you
                       will be prompted for the password.
 <cr>

ArubaOS-Switch(config)# snmpv3 user test auth ?
 AUTHENTICATION PASSWORD Set authentication password.
 md5                   Set the authentication protocol to md5.
 sha                   Set the authentication protocol to sha.

ArubaOS-Switch(config)# snmpv3 user test auth md5 ?
 AUTHENTICATION PASSWORD Set authentication password.

ArubaOS-Switch(config)# snmpv3 user test auth md5 password ?
 priv                  Specify Privacy password. If in enhanced secure-mode, you will be
                       prompted for the password.
 <cr>

ArubaOS-Switch(config)# snmpv3 user test auth md5 password priv ?
 PRIVACY PASSWORD      Specify Privacy password.
 des                   Set the privacy protocol to des.
 aes                   Set the privacy protocol to aes-128.

ArubaOS-Switch(config)# snmpv3 user test auth md5 password priv des ?
 PRIVACY PASSWORD      Specify Privacy password.

ArubaOS-Switch(config)# snmpv3 user test auth md5 password priv des password ?
 <cr>

ArubaOS-Switch(config)# snmpv3 user test auth md5 password priv des password


ArubaOS-Switch(config)# snmpv3 group ?
 managerpriv           Require privacy and authentication, can access all objects.
 managerauth           Require authentication, can access all objects.
 operatorauth          Requires authentication, limited access to objects.
 operatornoauth        No authentication required, limited access to objects.
 commanagerrw          Community with manager and unrestricted write access.
 commanagerr           Community with manager and restricted write access.
 comoperatorrw         Community with operator and unrestricted write access.
 comoperatorr          Community with operator and restricted write access.

ArubaOS-Switch(config)# snmpv3 group managerpriv ?
 user                  Set user to be added to the group.

ArubaOS-Switch(config)# snmpv3 group managerpriv user ?
 ASCII-STR             Enter an ASCII string.
```

```
ArubaOS-Switch(config)# snmpv3 group managerpriv user test ?
 sec-model             Set security model to be used.

ArubaOS-Switch(config)# snmpv3 group managerpriv user test sec-model ?
 ver1                  SNMP version 1 security model.
 ver2c                 SNMP version v2c security model.
 ver3                  SNMP version 3 security model.

ArubaOS-Switch(config)# snmpv3 group managerpriv user test sec-model ver3 ?
 <cr>

ArubaOS-Switch(config)# snmpv3 group managerpriv user test sec-model ver3


ArubaOS-Switch(config)# snmpv3 targetaddress ?
 ASCII-STR             Enter an ASCII string.

ArubaOS-Switch(config)# snmpv3 targetaddress NMS ?
 params                Set parameter name.

ArubaOS-Switch(config)# snmpv3 targetaddress NMS params ?
 ASCII-STR             Enter an ASCII string.

ArubaOS-Switch(config)# snmpv3 targetaddress NMS params all ?
 IP-ADDR               Set IP address of the destination target.
 IPV6-ADDR             Set IPv6 address of the destination target.

ArubaOS-Switch(config)# snmpv3 targetaddress NMS params all 10.0.111.210 ?
 addr-mask             Set range of transport addresses with this mask.
 filter                Set log filters.
 max-msg-size          Set maximum message size value; default is 1472.
 oobm                  Use OOBM interface to connect to server
 port-mask             Set range of udp ports with this mask.
 retries               Set retries value; default is 3.
 taglist               Set list of values used to select this entry from snmpNotifyTable.
 timeout               Set time-out value; default is 1500.
 udp-port              Set UDP port number to which the messages are sent; default is
                       162.
 <cr>

ArubaOS-Switch(config)# snmpv3 targetaddress NMS params all 10.0.111.210


ArubaOS-Switch(config)# snmp-server location
 ASCII-STR             Enter an ASCII string.

ArubaOS-Switch(config)# snmp-server location Lab

ArubaOS-Switch(config)# snmp-server contact
 ASCII-STR             Enter an ASCII string.

ArubaOS-Switch(config)# snmp-server contact Lab_Engr


ArubaOS-Switch# show snmpv3 enable

 Status and Counters - SNMP v3 Global Configuration Information

  SNMP v3 enabled : Yes

ArubaOS-Switch# show snmpv3 targetaddress
```

```
 snmpTargetAddrTable [rfc2573]

  Target Name                IP Address             Parameter
  -------------------------- ---------------------- ----------------------------
  NMS                        10.0.111.210           all


ArubaOS-Switch# show snmpv3 user

 Status and Counters - SNMP v3 Global Configuration Information

  User Name                        Auth. Protocol   Privacy Protocol
  -------------------------------- ---------------- ----------------
  initial                          SHA              CBC DES
  test                             MD5              CBC DES


ArubaOS-Switch# show snmpv3 group

 Status and Counters - SNMP v3 Global Configuration Information

  Security Name                  Security Model Group Name
  ------------------------------ -------------- --------------------------------
  CommunityManagerReadOnly       ver1           ComManagerR
  CommunityManagerReadWrite      ver1           ComManagerRW
  CommunityOperatorReadOnly      ver1           ComOperatorR
  CommunityOperatorReadWrite     ver1           ComOperatorRW
  CommunityManagerReadOnly       ver2c          ComManagerR
  CommunityManagerReadWrite      ver2c          ComManagerRW
  CommunityOperatorReadOnly      ver2c          ComOperatorR
  CommunityOperatorReadWrite     ver2c          ComOperatorRW
  test                           ver3           ManagerPriv
```

Comware5

[SNMP v3 is default enabled version]

(Note, if SNMP v1 & v2c has been configured and now only v3 is required, undo v1 v2c using this command `undo snmp-agent sys-info version v1 v2c` , and configure v3)

```
[Comware5]snmp-agent sys-info version v3


[Comware5]snmp-agent group ?
  v1   SNMPv1 security mode specified for this group name
  v2c  SNMPv2c security mode specified for this group name
  v3   USM(SNMPv3) security mode specified for this group name

[Comware5]snmp-agent group v3 ?
  STRING<1-32>  Group name

[Comware5]snmp-agent group v3 managerpriv ?
  acl             Set access control list for this group
  authentication  Specify a securityLevel of AuthNoPriv for this group name
  notify-view     Set a notify view for this group name
  privacy         Specify a securityLevel of AuthPriv for this group name
  read-view       Set a read view for this group name
  write-view      Set a write view for this group name
  <cr>

[Comware5]snmp-agent group v3 managerpriv privacy ?
  acl          Set access control list for this group
```

```
  notify-view  Set a notify view for this group name
  read-view    Set a read view for this group name
  write-view   Set a write view for this group name
  <cr>

[Comware5]snmp-agent group v3 managerpriv privacy


[Comware5]snmp-agent usm-user ?
  v1   SNMPv1 security model
  v2c  SNMPv2c security model
  v3   USM(SNMPv3) security model

[Comware5]snmp-agent usm-user v3 ?
  STRING<1-32>  User name

[Comware5]snmp-agent usm-user v3 test ?
  STRING<1-32>  The string of group to which the specified user belongs

[Comware5]snmp-agent usm-user v3 test managerpriv ?
  acl                  Set access control list for this user
  authentication-mode  Specify the authentication mode for the user
  cipher               Use secret key as password
  <cr>

[Comware5]snmp-agent usm-user v3 test managerpriv authentication-mode ?
  md5  Authenticate with HMAC MD5 algorithm
  sha  Authenticate with HMAC SHA algorithm

[Comware5]snmp-agent usm-user v3 test managerpriv authentication-mode md5 ?
  STRING<1-64>  Plain password of user authentication

[Comware5]snmp-agent usm-user v3 test managerpriv authentication-mode md5 password ?
  acl           Set access control list for this user
  privacy-mode  Specify the privacy mode for the user
  <cr>

[Comware5]snmp-agent usm-user v3 test managerpriv authentication-mode md5 password privacy-
mode ?
  3des    Use the 3DES encryption algorithm
  aes128  Use the 128bits AES encryption algorithm
  des56   Use the 56bits DES encryption algorithm

[Comware5]snmp-agent usm-user v3 test managerpriv authentication-mode md5 password privacy-
mode des ?
  STRING<1-64>  Plain password of user encryption

[Comware5]snmp-agent usm-user v3 test managerpriv authentication-mode md5 password privacy-
mode des password ?
  acl   Set access control list for this user
  <cr>

[Comware5]snmp-agent usm-user v3 test managerpriv authentication-mode md5 password privacy-
mode des password


[Comware5]snmp-agent target-host ?
  trap  Specify trap host target

[Comware5]snmp-agent target-host trap ?
  address  Specify the transport addresses to be used in the generation of SNMP
           messages
```

```
[Comware5]snmp-agent target-host trap address ?
  udp-domain  Specify transport domain over UDP for the target host

[Comware5]snmp-agent target-host trap address udp-domain ?
  STRING<1-255>  IP address or hostname of target host
  ipv6           Specify an ipv6 address as the target host address

[Comware5]snmp-agent target-host trap address udp-domain 10.0.111.210 ?
  dscp          Differentiated Services Codepoint (DSCP)
  params        Specify SNMP target information to be used in the generation of
                SNMP messages
  udp-port      Set port to receive traps/notifications for this target host
  vpn-instance  Specify VPN instance

[Comware5]snmp-agent target-host trap address udp-domain 10.0.111.210 params ?
  securityname  Specify the name for the principal on whose behalf SNMP
                messages will be generated

[Comware5]snmp-agent target-host trap address udp-domain 10.0.111.210 params securityname ?
  STRING<1-32>  Specify the character string of security name

[Comware5]snmp-agent target-host trap address udp-domain 10.0.111.210 params securityname
test ?
  v1    Specify security model of SNMPv1 to generate SNMP messages
  v2c   Specify security model of SNMPv2c to generate SNMP messages
  v3    Specify security model of SNMPv3 to generate SNMP messages
  <cr>

[Comware5]snmp-agent target-host trap address udp-domain 10.0.111.210 params securityname
test v3 ?
  authentication  Specify the securityLevel of AuthNoPriv
  privacy         Specify the securityLevel of AuthPriv
  <cr>

[Comware5]snmp-agent target-host trap address udp-domain 10.0.111.210 params securityname
test v3 privacy ?
  <cr>

[Comware5]snmp-agent target-host trap address udp-domain 10.0.111.210 params securityname
test v3 privacy


[Comware5]snmp-agent sys-info location ?
  TEXT  The physical location of this node<1-255>

[Comware5]snmp-agent sys-info location Lab

[Comware5]snmp-agent sys-info contact ?
  TEXT  Contact person information for this node<1-255>

[Comware5]snmp-agent sys-info contact Lab_Engr


[Comware5]display snmp-agent sys-info
   The contact person for this managed node:
           LabEngr

   The physical location of this node:
           Lab

   SNMP version running in the system:
           SNMPv3
```

```
[Comware5]display snmp-agent group

   Group name: managerpriv
       Security model: v3 AuthPriv
       Readview: ViewDefault
       Writeview: <no specified>
       Notifyview: <no specified>
       Storage-type: nonVolatile

[Comware5]display snmp-agent usm-user
   User name: test
   Group name: managerpriv
       Engine ID: 800063A203002389D5A070
       Storage-type: nonVolatile
       UserStatus: active
```

Comware7

[SNMP v3 is default enabled version]

(Note, if SNMP v1 & v2c has been configured and now only v3 is required, undo v1 v2c using this command `undo snmp-agent sys-info version v1 v2c` , and configure v3)

```
[Comware7]snmp-agent sys-info version v3


[Comware7]snmp-agent group ?
  v1   Specify SNMPv1 security mode for the group
  v2c  Specify SNMPv2c security mode for the group
  v3   Specify SNMPv3 security mode for the group

[Comware7]snmp-agent group v3 ?
  STRING<1-32>  Group name

[Comware7]snmp-agent group v3 managerpriv ?
  acl             Apply a basic ACL to filter NMSs
  authentication  Set the security level to AuthNoPriv
  notify-view     Specify notify views for the group
  privacy         Set the security level to AuthPriv
  read-view       Specify read views for the group
  write-view      Specify write views for the group
  <cr>

[Comware7]snmp-agent group v3 managerpriv privacy ?
  acl          Apply a basic ACL to filter NMSs
  notify-view  Specify notify views for the group
  read-view    Specify read views for the group
  write-view   Specify write views for the group
  <cr>

[Comware7]snmp-agent group v3 managerpriv privacy


[Comware7]snmp-agent usm-user ?
  v1   SNMPv1 security model
  v2c  SNMPv2c security model
  v3   SNMPv3 security model

[Comware7]snmp-agent usm-user v3 ?
  STRING<1-32>  Username

[Comware7]snmp-agent usm-user v3 test ?
  STRING<1-32>  Group name
```

```
  user-role     Specify the role of the SNMPv3 user

[Comware7]snmp-agent usm-user v3 test managerpriv ?
  acl     Set access control list for this user
  cipher  Specify a ciphertext key
  remote  Specify the remote engine associated with the user
  simple  Specify a plaintext key
  <cr>

[Comware7]snmp-agent usm-user v3 test managerpriv simple ?
  authentication-mode  Specify an authentication algorithm

[Comware7]snmp-agent usm-user v3 test managerpriv simple authentication-mode ?
  md5  Use the HMAC MD5 authentication algorithm
  sha  Use the HMAC SHA authentication algorithm

[Comware7]snmp-agent usm-user v3 test managerpriv simple authentication-mode md5 ?
  STRING<1-64>  Plaintext key string

[Comware7]snmp-agent usm-user v3 test managerpriv simple authentication-mode md5 password ?
  acl           Set access control list for this user
  privacy-mode  Specify an encryption algorithm for privacy
  <cr>

[Comware7]snmp-agent usm-user v3 test managerpriv simple authentication-mode md5 password
privacy-mode ?
  3des    Use the 3DES encryption algorithm
  aes128  Use the 128-bit AES encryption algorithm
  des56   Use the 56-bit DES encryption algorithm

[Comware7]snmp-agent usm-user v3 test managerpriv simple authentication-mode md5 password
privacy-mode des ?
  STRING<1-64>  Plaintext key string

[Comware7]snmp-agent usm-user v3 test managerpriv simple authentication-mode md5 password
privacy-mode des password ?
  acl   Set access control list for this user
  <cr>

[Comware7]snmp-agent usm-user v3 test managerpriv simple authentication-mode md5 password
privacy-mode des password


[Comware7]snmp-agent target-host ?
  inform  Set a target host to receive SNMP informs
  trap    Set a target host to receive SNMP traps

[Comware7]snmp-agent target-host trap ?
  address  Specify the transport address of the target host

[Comware7]snmp-agent target-host trap address ?
  udp-domain  Use UDP to transport SNMP information

[Comware7]snmp-agent target-host trap address udp-domain ?
  STRING<1-253>  IP address or hostname of the target host
  ipv6           IPv6 address of the target host

[Comware7]snmp-agent target-host trap address udp-domain 10.0.111.210 ?
  params        Specify SNMP information to be used in the generation of SNMP
                notifications
  udp-port      Set port to receive notifications for the target host
  vpn-instance  Specify VPN instance
```

```
[Comware7]snmp-agent target-host trap address udp-domain 10.0.111.210 params ?
  securityname  Specify the security name for the principal on whose behalf SNMP
                notifications will be generated

[Comware7]snmp-agent target-host trap address udp-domain 10.0.111.210 params securityname ?
  STRING<1-32>  Security name

[Comware7]snmp-agent target-host trap address udp-domain 10.0.111.210 params securityname
test ?
  v1    Set the security model to SNMPv1 for generating SNMP notifications
  v2c   Set the security model to SNMPv2 for generating SNMP notifications
  v3    Set the security model to SNMPv3 for generating SNMP notifications
  <cr>

[Comware7]snmp-agent target-host trap address udp-domain 10.0.111.210 params securityname
test v3 ?
  authentication  Set the security level to AuthNoPriv
  privacy         Set the security level to AuthPriv
  <cr>

[Comware7]snmp-agent target-host trap address udp-domain 10.0.111.210 params securityname
test v3 privacy ?
  <cr>

[Comware7]snmp-agent target-host trap address udp-domain 10.0.111.210 params securityname
test v3 privacy


[Comware7]snmp-agent sys-info location ?
  TEXT  Location information of the agent, 1 to 255 characters

[Comware7]snmp-agent sys-info location Lab

[Comware7]snmp-agent sys-info contact ?
  TEXT  Contact information, 1 to 255 characters

[Comware7]snmp-agent sys-info contact Lab_Engr


[Comware7]display snmp-agent sys-info
  The contact information of the agent:
      Lab_Engr

  The location information of the agent:
      Lab

  The SNMP version of the agent:
      SNMPv3

[Comware7]display snmp-agent group
   Group name: managerpriv
       Security model: v3 AuthPriv
       Readview: ViewDefault
       Writeview: <no specified>
       Notifyview: <no specified>
       Storage-type: nonVolatile

[Comware7]display snmp-agent usm-user
   Username: test
   Group name: managerpriv
       Engine ID: 800063A280CC3E5F73BACF00000001
       Storage-type: nonVolatile
       UserStatus: active
```

Cisco

```
Cisco(config)#snmp-server group ?
  WORD  Name of the group

Cisco(config)#snmp-server group managerpriv ?
  v1   group using the v1 security model
  v2c  group using the v2c security model
  v3   group using the User Security Model (SNMPv3)

Cisco(config)#snmp-server group managerpriv v3 ?
  auth    group using the authNoPriv Security Level
  noauth  group using the noAuthNoPriv Security Level
  priv    group using SNMPv3 authPriv security level

Cisco(config)#snmp-server group managerpriv v3 priv ?
  access   specify an access-list associated with this group
  context  specify a context to associate these views for the group
  match    context name match criteria
  notify   specify a notify view for the group
  read     specify a read view for the group
  write    specify a write view for the group
  <cr>

Cisco(config)#snmp-server group managerpriv v3 priv


Cisco(config)#snmp-server user ?
  WORD  Name of the user

Cisco(config)#snmp-server user test ?
  WORD  Group to which the user belongs

Cisco(config)#snmp-server user test managerpriv ?
  remote  Specify a remote SNMP entity to which the user belongs
  v1      user using the v1 security model
  v2c     user using the v2c security model
  v3      user using the v3 security model

Cisco(config)#snmp-server user test managerpriv v3 ?
  access     specify an access-list associated with this group
  auth       authentication parameters for the user
  encrypted  specifying passwords as MD5 or SHA digests
  <cr>

Cisco(config)#snmp-server user test managerpriv v3 auth ?
  md5  Use HMAC MD5 algorithm for authentication
  sha  Use HMAC SHA algorithm for authentication

Cisco(config)#snmp-server user test managerpriv v3 auth md5 ?
  WORD  authentication password for user

Cisco(config)#snmp-server user test managerpriv v3 auth md5 password ?
  access  specify an access-list associated with this group
  priv    encryption parameters for the user
  <cr>

Cisco(config)#snmp-server user test managerpriv v3 auth md5 password priv ?
  3des  Use 168 bit 3DES algorithm for encryption
  aes   Use AES algorithm for encryption
  des   Use 56 bit DES algorithm for encryption

Cisco(config)#snmp-server user test managerpriv v3 auth md5 password priv des ?
```

```
  WORD  privacy pasword for user

Cisco(config)#snmp-server user test managerpriv v3 auth md5 password priv des password ?
  access  specify an access-list associated with this group
  <cr>

Cisco(config)#snmp-server user test managerpriv v3 auth md5 password priv des password


Cisco(config)#snmp-server host ?
  WORD                                                IP/IPV6 address of SNMP
                                                      notification host
  http://<Hostname or A.B.C.D>[:<port number>][/<uri>]  HTTP address of XML
                                                      notification host

Cisco(config)#snmp-server host 10.0.111.210 ?
  WORD     SNMPv1/v2c community string or SNMPv3 user name
  informs  Send Inform messages to this host
  traps    Send Trap messages to this host
  version  SNMP version to use for notification messages
  vrf      VPN Routing instance for this host

Cisco(config)#snmp-server host 10.0.111.210 version ?
  1   Use SNMPv1
  2c  Use SNMPv2c
  3   Use SNMPv3

Cisco(config)#snmp-server host 10.0.111.210 version 3 ?
  auth    Use the SNMPv3 authNoPriv Security Level
  noauth  Use the SNMPv3 noAuthNoPriv Security Level
  priv    Use the SNMPv3 authPriv Security Level

Cisco(config)#snmp-server host 10.0.111.210 version 3 priv ?
  WORD  SNMPv1/v2c community string or SNMPv3 user name

Cisco(config)#snmp-server host 10.0.111.210 version 3 priv test ?
  auth-framework    Allow SNMP CISCO-AUTH-FRAMEWORK-MIB traps
  bridge            Allow SNMP STP Bridge MIB traps
  call-home         Allow SNMP CISCO-CALLHOME-MIB traps
  cef               Allows cef traps
  cluster           Allow Cluster Member Status traps
  config            Allow SNMP config traps
  config-copy       Allow SNMP config-copy traps
  config-ctid       Allow SNMP config-ctid traps
  copy-config       Allow SNMP copy-config traps
  cpu               Allow cpu related traps
  dot1x             Allow dot1x traps
  eigrp             Allow SNMP EIGRP traps
  energywise        Allow SNMP energywise traps
  entity            Allow SNMP entity traps
  envmon            Allow environmental monitor traps
  errdisable        Allow errordisable notifications
  event-manager     Allow SNMP Embedded Event Manager traps
  flash             Allow SNMP FLASH traps
  flowmon           Allow SNMP flow monitor notifications
  fru-ctrl          Allow entity FRU control traps
  hsrp              Allow SNMP HSRP traps
  ipmulticast       Allow SNMP ipmulticast traps
  ipsla             Allow SNMP Host IP SLA traps
  license           Allow license traps
  mac-notification  Allow SNMP MAC Notification Traps
  ospf              Allow OSPF traps
  pim               Allow SNMP PIM traps
```

```
  port-security     Allow SNMP port-security traps
  power-ethernet    Allow SNMP power ethernet traps
  snmp              Allow SNMP-type notifications
  stackwise         Allow SNMP stackwise traps
  storm-control     Allow SNMP storm-control traps
  stpx              Allow SNMP STPX MIB traps
  syslog            Allow SNMP syslog traps
  tty               Allow TCP connection traps
  udp-port          The notification host's UDP port number (default port 162)
  vlan-membership   Allow SNMP VLAN membership traps
  vlancreate        Allow SNMP VLAN created traps
  vlandelete        Allow SNMP VLAN deleted traps
  vstack            Allow SNMP Smart Install traps
  vtp               Allow SNMP VTP traps
  <cr>

Cisco(config)#snmp-server host 10.0.111.210 version 3 priv test


Cisco(config)#snmp-server location ?
  LINE  The physical location of this node

Cisco(config)#snmp-server location Lab

Cisco(config)#snmp-server contact ?
  LINE  identification of the contact person for this managed node

Cisco(config)#snmp-server contact Lab_Engr


Cisco#show snmp host
Notification host: 10.0.111.210 udp-port: 162   type: trap
user: test      security model: v3 priv


Cisco#show snmp user

User name: test
Engine ID: 800000090300002291AB4381
storage-type: nonvolatile        active
Authentication Protocol: MD5
Privacy Protocol: DES
Group-name: managerpriv


Cisco#show snmp group
groupname: managerpriv                      security model:v3 priv
readview : v1default                        writeview: <no writeview specified>
notifyview: *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F
row status: active
```

Chapter 8 CLI Management Access – Telnet and SSH

This chapter compares the commands you use to enable and configure Telnet and Secure Shell (SSH) services for device management via unencrypted and encrypted network access.

Note: ssh on Comware does not support 'authentication-mode password' on vty interfaces and must be configured for 'authentication-mode scheme'.

Note: ssh on Cisco does not support 'local' (password only) on vty interfaces and must be configured for 'login local'.

You can find configuration details for User ID's and Password's in Chapter 2.

a) Telnet

ArubaOS-Switch	Comware5	Cisco
Telnet is enabled by default and is available as soon as an IP addr is assigned to a VLAN, without UID/PW access control. To control access with UID/PW or PW (only), see Ch2 for configuring UID/PW or PW only.	telnet is disabled by default, requires: 1) enable telnet server 2) configuration on the vty interface(s) 3) 'authentication-mode password' is default configuration, but no password is configured Must configure uid/pw if 'authentication-mode scheme' is used, see Ch2. If authentication-mode 'scheme' is used, user must have 'service-type telnet' configured.	Must config vty login scheme local or password to activate telnet capability. If 'login' is used, enable password must be configured, see Ch2. If 'login local' is used, uid/pw must be configured, see Ch2.
	`[Comware5]telnet server enable`	

	`[Comware5]local-user <name>`
	
	`[Comware5-luser-manager]service-type telnet`	

	`[Comware5]user-interface vty 0 15`
	
	`[Comware5-ui-vty0-15]authentication-mode scheme`
		`Cisco(config)#line vty 0 15`
		
		`Cisco(config-line)#login local`

	`[Comware5]user-interface vty 0 15`
	
	`[Comware5-ui-vty0-15]authentication-mode password`
		`Cisco(config)#line vty 0 15`
		
		`Cisco(config-line)#login`
		
		`Cisco(config-line)#password 0 password`

	[Comware5-ui-vty0-15]user privilege level 3 [Comware5-ui-vty0-15]set authentication password simple password	
	Comware7	
	[Comware7]telnet server enable	
	[Comware7]local-user <name> [Comware7-luser-manager]service-type telnet	
	[Comware7]user-interface vty 0 63 [Comware7-ui-vty0-63]authentication-mode scheme	
	[Comware7]user-interface vty 0 63 [Comware7-ui-vty0-63]authentication-mode password [Comware7-line-vty0-63]user-role network-admin [Comware7-ui-vty0-63]set authentication password simple password	
ArubaOS-Switch# show telnet	[Comware]display users	Cisco#show users
	[Comware]display users all	

ArubaOS-Switch

Telnet is enabled by default and is available as soon as an IP addr is assigned to a VLAN, without UID/PW access control.

To control access with UID/PW or PW (only), see Ch2 for configuring UID/PW or PW only.

```
ArubaOS-Switch# show telnet

 Telnet Activity

 Source IP Selection: 10.0.111.21

 -------------------------------------------------------
 Session  :     1
 Privilege: Manager
 From     : Console
 To       :
 -------------------------------------------------------
 Session  : **  2
 Privilege: Manager
 From     : 10.0.100.80
 To       :
```

Comware5

```
[Comware5]telnet ?
  client  Specify TELNET client attribute
  server  TELNET server functions

[Comware5]telnet server ?
  acl     Specify an ACL to control telnet clients' access
  dscp    Differentiated Services Codepoint (DSCP)
  enable  Enable TELNET server functions
  ipv6    Specify IPv6 attribute

[Comware5]telnet server enable


[Comware5]local-user <name>

[Comware5-luser-manager]service-type ?
  ftp         FTP service type
  lan-access  LAN-ACCESS service type
  portal      Portal service type
  ssh         Secure Shell service type
  telnet      TELNET service type
  terminal    TERMINAL service type
  web         Web service type

[Comware5-luser-manager]service-type telnet


[the next command sets the use of uid/pw for login via vty]

[Comware5]user-interface vty 0 15

[Comware5-ui-vty0-15]authentication-mode ?
  none      Login without checking
  password  Authentication use password of user terminal interface
  scheme    Authentication use AAA

[Comware5-ui-vty0-15]authentication-mode scheme ?
  <cr>

[Comware5-ui-vty0-15]authentication-mode scheme


[the next command sets the use of password only for login via vty]

[Comware5]user-interface vty 0 15

[Comware5-ui-vty0-15]authentication-mode password

[Comware5-ui-vty0-15]user ?
  privilege  Specify the login priority of user terminal interface

[Comware5-ui-vty0-15]user privilege ?
  level  Specify the privilege level of user interface

[Comware5-ui-vty0-15]user privilege level ?
  INTEGER<0-3>  Specify privilege level

[Comware5-ui-vty0-15]user privilege level 3 ?
  <cr>
```

```
[Comware5-ui-vty0-15]user privilege level 3

[Comware5-ui-vty0-15]set authentication ?
  password  Specify the password of user interface

[Comware5-ui-vty0-15]set authentication password ?
  cipher  Set the password with cipher text
  hash    Save and display the hash value of the password
  simple  Set the password with plain text

[Comware5-ui-vty0-15]set authentication password simple ?
  STRING<1-16>  Plain text password

[Comware5-ui-vty0-15]set authentication password simple password ?
  <cr>

[Comware5-ui-vty0-15]set authentication password simple password


[Comware5]display users
The user application information of the user interface(s):
  Idx UI      Delay    Type Userlevel
  0   AUX 0   00:00:40      3
+ 25  VTY 0   00:00:00 TEL  3

Following are more details.
AUX 0   :
        User name: manager
VTY 0   :
        User name: manager
        Location: 10.0.100.80
 +    : Current operation user.
 F    : Current operation user work in async mode.

[Comware5]display users all
The user application information of all user interfaces:
  Idx UI      Delay    Type Userlevel
F 0   AUX 0   00:00:00      3
+ 25  VTY 0   00:03:11 TEL  3
  26  VTY 1
  27  VTY 2
  28  VTY 3
  29  VTY 4
  30  VTY 5
  31  VTY 6
  32  VTY 7
  33  VTY 8
  34  VTY 9
  35  VTY 10
  36  VTY 11
  37  VTY 12
  38  VTY 13
  39  VTY 14
  40  VTY 15

Following are more details.
AUX 0   :
        User name: manager
VTY 0   :
        User name: manager
        Location: 10.0.100.80
 +    : User-interface is active.
 F    : User-interface is active and work in async mode.
```

Comware7

```
[Comware7]telnet ?
  client  Specify telnet client attribute
  server  Telnet server configuration

[Comware7]telnet server ?
  acl     Specify an ACL to control telnet clients' access
  dscp    Set the Differentiated Services Codepoint (DSCP) value
  enable  Enable telnet server function
  ipv6    IPv6 information

[Comware7]telnet server enable


[Comware7]local-user <name>

[Comware7-luser-manage-manager]service-type ?
  ftp       FTP service
  http      HTTP service type
  https     HTTPS service type
  pad       X.25 PAD service
  ssh       Secure Shell service
  telnet    Telnet service
  terminal  Terminal access service

[Comware7-luser-manager]service-type telnet


[the next command sets the use of uid/pw for login via vty]

[Comware7]user-interface vty 0 63

[Comware7-line-vty0-63]authentication-mode ?
  none      Login without authentication
  password  Password authentication
  scheme    Authentication use AAA

[Comware7-line-vty0-63]authentication-mode scheme ?
  <cr>

[Comware7-line-vty0-63]authentication-mode scheme


[the next command sets the use of password only for login via vty]

[Comware7]user-interface vty 0 63

[Comware7-line-vty0-63]authentication-mode password


[Comware7-line-vty0-63]user-role ?
  STRING<1-63>      User role name
  network-admin
  network-operator
  level-0
  level-1
  level-2
  level-3
  level-4
  level-5
  level-6
  level-7
```

```
  level-8
  level-9
  level-10
  level-11
  level-12
  level-13
  level-14
  level-15
  security-audit

[Comware7-line-vty0-63]user-role network-admin ?
  <cr>

[Comware7-line-vty0-63]user-role network-admin


[Comware7-line-vty0-63]set authentication ?
  password  Specify the password of line

[Comware7-line-vty0-63]set authentication password ?
  hash    Specify a hashtext password
  simple  Specify a plaintext password

[Comware7-line-vty0-63]set authentication password simple ?
  STRING<1-16>  Plaintext password string

[Comware7-line-vty0-63]set authentication password simple password ?
  <cr>

[Comware7-line-vty0-63]set authentication password simple password


[Comware7]display users
  Idx  Line    Idle       Time              Pid     Type
F 0    AUX 0   00:00:00   Mar 26 17:12:50   436
  129  VTY 0   00:00:38   Mar 26 17:35:18   500     TEL

Following are more details.
VTY 0   :
        Location: 10.0.100.84
 +    : Current operation user.
 F    : Current operation user works in async mode.

[Comware7]display users all
  Idx  Line    Idle       Time              Pid     Type
F 0    AUX 0   00:00:00   Mar 26 17:12:50   436
+ 129  VTY 0   00:01:03   Mar 26 17:35:18   500     TEL
  130  VTY 1
  131  VTY 2
  132  VTY 3
  133  VTY 4
  134  VTY 5
  135  VTY 6
  136  VTY 7
  137  VTY 8
  138  VTY 9
  139  VTY 10
  ...
  189  VTY 60
  190  VTY 61
  191  VTY 62
  192  VTY 63
```

```
Following are more details.
VTY 0   :
        Location: 10.0.100.84
 +    : Line is active.
 F    : Line is active and works in async mode.
```

Cisco

```
Cisco(config)#line vty 0 15

Cisco(config-line)#login ?
  local   Local password checking
  <cr>
```

[the next command sets the use of user-id & password (locally configured) for login via vty]

```
Cisco(config-line)#login local ?
  <cr>

Cisco(config-line)#login local
```

[the next command sets the use of password only for login via vty]

```
Cisco(config)#line vty 0 15

Cisco(config-line)#login


Cisco(config-line)#password ?
  0     Specifies an UNENCRYPTED password will follow
  7     Specifies a HIDDEN password will follow
  LINE  The UNENCRYPTED (cleartext) line password

Cisco(config-line)#password 0 ?
  LINE  The UNENCRYPTED (cleartext) line password

Cisco(config-line)#password 0 password ?
LINE    <cr>

Cisco(config-line)#password 0 password


Cisco#show users
    Line       User       Host(s)              Idle       Location
*  0 con 0     manager    idle                 00:00:00
   1 vty 0                idle                 00:00:14 10.0.100.84

  Interface    User               Mode         Idle     Peer Address
```

b) SSH

ArubaOS-Switch	Comware5	Cisco
		Cisco(config)#hostname Cisco
		Cisco(config)#ip domain-name test
ArubaOS-Switch(config)# crypto key generate ssh	[Comware5]public-key local create rsa	Cisco(config)#crypto key generate
ArubaOS-Switch(config)# ip ssh	[Comware5]ssh server enable	Cisco(config)#ip ssh version 2
	[Comware5]user-interface vty 0 15 [Comware5-ui-vty0-15]authentication-mode scheme [Comware5-ui-vty0-15]protocol inbound ssh	Cisco(config)#line vty 0 15 Cisco(config-line)#login local Cisco(config-line)#transport input ssh
	[Comware5]local-user <name> [Comware5-luser-ssh-manager]password simple password [Comware5-luser-ssh-manager]service-type ssh [Comware5-luser-ssh-manager]authorization-attribute level 3	Cisco(config)#username <name> privilege 15 password <password>
ArubaOS-Switch(config)# no telnet-server	[Comware5]undo telnet server enable	(NOTE: by configuring 'transport input ssh' on the vty interfaces, telnet access is disabled)
	Comware7	
	[Comware7]public-key local create rsa	
	[Comware7]ssh server enable	
	[Comware7]user-interface vty 0 63 [Comware7-ui-vty0-63]authentication-mode scheme [Comware7-ui-vty0-63]protocol inbound ssh	
	[Comware7]local-user <name> [Comware7-luser-ssh-manager]password simple password [Comware7-luser-ssh-manager]service-type ssh [Comware7-luser-manage-ssh-manager]authorization-attribute user-role network-adm in	
	[Comware7]undo telnet server enable	

ArubaOS-Switch# show ip ssh	[Comware]display ssh server status [Comware]display ssh server session	Cisco#show ip ssh Cisco#show ssh
ArubaOS-Switch# show crypto host-public-key	[Comware]display public-key local rsa public	Cisco#show crypto key mypubkey rsa
ArubaOS-Switch# show ip host-public-key		

ArubaOS-Switch

```
ArubaOS-Switch(config)# crypto ?
key                    Install/remove RSA key file for ssh.
 pki                    Public Key Infrastructure management

ArubaOS-Switch(config)# crypto key ?
 generate               Generate a new key.
 zeroize                Delete existing key.

ArubaOS-Switch(config)# crypto key generate ?
 autorun-key            Install RSA key file for autorun
 ssh                    Install host key file for ssh server.

ArubaOS-Switch(config)# crypto key generate ssh ?
 dsa                    Install DSA host key.
 rsa                    Install RSA host key.
 <cr>

ArubaOS-Switch(config)# crypto key generate ssh
Installing new key pair.  If the key/entropy cache is
depleted, this could take up to a minute.


ArubaOS-Switch(config)# ip ssh ?
 cipher                 Specify a cipher to enable/disable.
 filetransfer           Enable/disable secure file transfer capability.
 listen                 Specify in which mode daemon should listen in.
 mac                    Specify a mac to enable/disable.
 port                   Specify the TCP port on which the daemon should listen for SSH
                        connections.
 public-key             Configure a client public-key.
 timeout                Specify the maximum length of time (seconds) permitted for
                        protocol negotiation and authentication.
 <cr>

ArubaOS-Switch(config)# ip ssh


ArubaOS-Switch(config)# no telnet-server


ArubaOS-Switch# show ip ssh


  SSH Enabled     : Yes                  Secure Copy Enabled : No
  TCP Port Number : 22                   Timeout (sec)       : 120
  Host Key Type   : RSA                  Host Key Size       : 2048

  Ciphers : aes256-ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-ctr,
            aes192-cbc,aes128-ctr,aes128-cbc,3des-cbc
```

```
  MACs    : hmac-sha1-96,hmac-md5,hmac-sha1,hmac-md5-96

  Ses Type     | Source IP                                      Port
  --- -------- + ---------------------------------------------- -----
  1   console  |
  2   telnet   |
  3   ssh      | 10.0.100.80                                    59987
  4   inactive |
  5   inactive |
  6   inactive |
  7   inactive |

ArubaOS-Switch# show crypto host-public-key

SSH host public key:

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA2tfJ6jJIdewRSD8D5YV8/wqWPLa0leK5VDBDBZeqmAIJ
GL7JQmO+N+WgPVvbIm8V20QCqR1WHVsVNUAE6O6ErFybfk098Y089HuA7v6ej8lTF9r0U0BMQuNLp5C4
++92wCh/mWJmwTUBIqY2w2tfq4rtNxap123456789054/6o5wIHHC8fNjUf5pwil+nxYOk/migsklDAG
CyH6OdUWWO2Rb2J/nouBOyz/VKLLuT4kO8LF728rxPBQfk7m/a3cKBKkSAM9O+cuTDzT1u3hOnc3zKGh
Q38nMfTPvCCQZLTljhGGywHl0uGxzHbSFShRyIRyIrMpvQtX85GcLcZLhw==

-or-

ArubaOS-Switch# show ip host-public-key

SSH host public key:

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA2tfJ6jJIdewRSD8D5YV8/wqWPLa0leK5VDBDBZeqmAIJ
GL7JQmO+N+WgPVvbIm8V20QCqR1WHVs123456789054Fybfk098Y0HuA7v6ej8lTF9r0U0BMQuNLp5C4
++92wCh/mWJmwTUBIqY2w2tfq4rtNxapHN+NTQAiPQIc/6o5wIHHC8fNjUf5pwil+nxYOk/migsklDAG
CyH6OdUWWO2Rb2J/nouBOyz/VKLLuT4kO8LF728rxPBQfk7m/a3cKBKkSAM9O+cuTDzT1u3hOnc3zKGh
Q38nMfTPvCCQZLTljhGGywHl0uGxzHbSFShRyIRyIrMpvQtX85GcLcZLhw==
```

Comware5

```
[Comware5]public-key ?
  local  Local public key pair operations
  peer   Peer public key configuration

[Comware5]public-key local ?
  create   Create new local key pair
  destroy  Destroy the local key pair
  export   Print or export the local key pair

[Comware5]public-key local create ?
  dsa    Key type DSA
  ecdsa  Key type ECDSA
  rsa    Key type RSA

[Comware5]public-key local create rsa ?
  <cr>

[Comware5]public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...

[Comware5]user-interface vty 0 15
```

```
[Comware5-ui-vty0-4]authentication-mode ?
  none      Login without checking
  password  Authentication use password of user terminal interface
  scheme    Authentication use AAA

[Comware5-ui-vty0-15]authentication-mode scheme ?
  <cr>

[Comware5-ui-vty0-15]authentication-mode scheme

[Comware5-ui-vty0-15]protocol ?
  inbound  Specify user interface incoming protocol

[Comware5-ui-vty0-15]protocol inbound ?
  all     All protocols
  ssh     SSH protocol
  telnet  Telnet protocol

[Comware5-ui-vty0-15]protocol inbound ssh ?
  <cr>

[Comware5-ui-vty0-15]protocol inbound ssh
```

NOTE: by configuring 'protocol inbound ssh' on the vty interfaces, if telnet access was previously enabled, it is now functionally disabled, however still remove the 'telnet server enable' command, as done later in a few steps.

```
[Comware5]local-user <name>

[Comware5-luser-ssh-manager]password simple password

[Comware5-luser-ssh-manager]service-type ?
  ftp         FTP service type
  lan-access  LAN-ACCESS service type
  portal      Portal service type
  ssh         Secure Shell service type
  telnet      TELNET service type
  terminal    TERMINAL service type
  web         Web service type

[Comware5-luser-ssh-manager]service-type ssh ?
  telnet    TELNET service type
  terminal  TERMINAL service type
  <cr>

[Comware5-luser-ssh-manager]service-type ssh

[Comware5-luser- ssh-manager]authorization-attribute ?
  acl              Specify ACL number of user
  callback-number  Specify dialing character string for callback user
  idle-cut         Specify idle-cut of local user
  level            Specify level of user
  user-profile     Specify user profile of user
  user-role        Specify role of local user
  vlan             Specify VLAN ID of user
  work-directory   Specify directory of user

[Comware5-luser- ssh-manager]authorization-attribute level ?
  INTEGER<0-3>  Level of user

[Comware5-luser- ssh-manager]authorization-attribute level 3 ?
  acl              Specify ACL number of user
  callback-number  Specify dialing character string for callback user
```

```
  idle-cut         Specify idle-cut of local user
  user-profile     Specify user profile of user
  user-role        Specify role of local user
  vlan             Specify VLAN ID of user
  work-directory   Specify directory of user
  <cr>

[Comware5-luser-ssh-manager]authorization-attribute level 3

[Comware5]undo telnet server enable


[Comware5]ssh ?
  client  Specify SSH client attribute
  server  Specify the server attribute
  user    SSH user

[Comware5]ssh server ?
  acl                     Specify an ACL to control SSH clients' access
  authentication-retries  Specify authentication retry times
  authentication-timeout  Specify authentication timeout
  compatible-ssh1x        Specify the compatible ssh1x
  dscp                    Differentiated Services Codepoint (DSCP)
  enable                  Enable SSH Server
  ipv6                    Specify SSH Server IPv6 attribute
  rekey-interval          Specify the SSH server key rekey-interval

[Comware5]ssh server enable ?
  <cr>

[Comware5]ssh server enable


[Comware5]display ssh server ?
  session  Server session
  status   Server state

[Comware5]display ssh server status

SSH server: Enable
 SSH version : 1.99
 SSH authentication-timeout : 60 second(s)
 SSH server key generating interval : 0 hour(s)
 SSH authentication retries : 3 time(s)
 SFTP server: Disable
 SFTP server Idle-Timeout: 10 minute(s)

[Comware5]display ssh server session
 Conn   Ver   Encry    State          Retry    SerType  Username
 VTY 0  2.0   AES      Established    0        Stelnet  ssh-manager


[Comware5]display public-key local rsa public

=====================================================
Time of Key pair created: 15:16:11  2015/03/12
Key name: HOST_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100BF156BF41CE4EB567EBA80D644E20A3339A
1EDC43701F758DFB89B72BCCFCC14123456789054AFC9EECB32D56A1E2D220BB7BDBB0FE9D6A46A79C21CA84BA04F
```

```
1EB1E9E57D60497A1EF1D536C3ED4B8468C48C77CBC7C56052D04A93552A0A7BCB98805F1EF8B29A6ABC4FFCA930E
1912A07506E629000CDEFC570E3106605C910203010001
=====================================================
Time of Key pair created: 15:16:18  2015/03/12
Key name: SERVER_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
307C300D06092A864886F70D0101010500036B003068026100C05DE56C3141015C6D792DDE419B436530E666C615E
339A09B3C189C4332AAEE575344966B0123456789054519F7BA917F95464B354BCD998AC0E49463334B8C6D4ADC55
CC4C77EE7201FCC80AD63979DC9DBD4EB525E3C53B0E3BAE54D33272BF0203010001
```

Comware7

```
[Comware7]public-key ?
  local  Local key pairs
  peer   Configure peer's public key

[Comware7]public-key local ?
  create   Create a local key pair
  destroy  Destroy local key pairs
  export   Print or export the public key

[Comware7]public-key local create ?
  dsa    DSA key pair
  ecdsa  ECDSA key pair
  rsa    RSA key pairs

[Comware7]public-key local create rsa ?
  name  Specify the name of the key pair
  <cr>

[Comware7]public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...


[Comware7]user-interface vty 0 63

[Comware7-line-vty0-63]authentication-mode ?
  none      Login without authentication
  password  Password authentication
  scheme    Authentication use AAA

[Comware7-line-vty0-63]authentication-mode scheme ?
  <cr>

[Comware7-line-vty0-63]authentication-mode scheme

[Comware7-line-vty0-63]protocol ?
  inbound  Incoming protocols

[Comware7-line-vty0-63]protocol inbound ?
  all     All protocols
  ssh     SSH protocol
  telnet  Telnet protocol

[Comware7-line-vty0-63]protocol inbound ssh ?
  <cr>
```

```
[Comware7-line-vty0-63]protocol inbound ssh


[Comware7]local-user <name>

[Comware7-luser-manage-ssh-manager]password simple password

[Comware7-luser-manage-ssh-manager]service-type ?
  ftp       FTP service
  http      HTTP service type
  https     HTTPS service type
  pad       X.25 PAD service
  ssh       Secure Shell service
  telnet    Telnet service
  terminal  Terminal access service

[Comware7-luser-manage-ssh-manager]service-type ssh ?
  http      HTTP service type
  https     HTTPS service type
  pad       X.25 PAD service
  telnet    Telnet service
  terminal  Terminal access service
  <cr>

[Comware7-luser-manage-ssh-manager]service-type ssh
```

NOTE: by configuring 'protocol inbound ssh' on the vty interfaces, if telnet access was previously enabled, it is now functionally disabled, however still remove the 'telnet server enable' command, as done later in a few steps.

```
[Comware7-luser-manage-ssh-manager]authorization-attribute ?
  acl              Specify ACL of local user
  callback-number  Specify PPP callback number of local user
  idle-cut         Specify idle cut function for local user
  user-profile     Specify user profile of local user
  user-role        Specify user role of the local user
  vlan             Specify VLAN ID of local user
  work-directory   Specify work directory of local user

[Comware7-luser-manage-ssh-manager]authorization-attribute user-role ?
  STRING<1-63>      User role name
  network-admin
  network-operator
  level-0
  level-1
  level-2
  level-3
  level-4
  level-5
  level-6
  level-7
  level-8
  level-9
  level-10
  level-11
  level-12
  level-13
  level-14
  level-15
  security-audit

[Comware7-luser-manage-ssh-manager]authorization-attribute user-role network-admin ?
  acl              Specify ACL of local user
```

```
  callback-number  Specify PPP callback number of local user
  idle-cut         Specify idle cut function for local user
  user-profile     Specify user profile of local user
  vlan             Specify VLAN ID of local user
  work-directory   Specify work directory of local user
  <cr>

[Comware7-luser-manage-ssh-manager]authorization-attribute user-role network-admin

[Comware7]undo telnet server enable


[Comware7]ssh ?
  client  SSH client configuration
  server  Specify the server attribute
  user    SSH user

[Comware7]ssh server ?
  acl                      Specify an ACL used to control the SSH clients' access
  authentication-retries   Specify authentication retry times
  authentication-timeout   Specify authentication timeout
  compatible-ssh1x         Enable compatible ssh1x
  dscp                     Set the Differentiated Services Codepoint (DSCP) value
  enable                   Enable Stelnet Server
  ipv6                     IPv6 information
  rekey-interval           Specify the SSH server key rekey-interval

[Comware7]ssh server enable ?
  <cr>

[Comware7]ssh server enable


[Comware7]display ssh server ?
  session  Server session
  status   Server state

[Comware7]display ssh server status
 Stelnet server: Enable
 SSH version : 1.99
 SSH authentication-timeout : 60 second(s)
 SSH server key generating interval : 0 hour(s)
 SSH authentication retries : 3 time(s)
 SFTP server: Disable
 SFTP Server Idle-Timeout: 10 minute(s)
 NETCONF server: Disable
 SCP server: Disable


[Comware7]display ssh server session
 UserPid   SessID Ver   Encrypt    State          Retries  Serv     Username
 583       0      2.0   aes256-cbc Established    0        Stelnet  ssh-manager


[Comware7]display public-key local rsa public

=============================================
Key name: hostkey(default)
Key type: RSA
Time when key pair created: 17:51:54 2015/03/26
Key code:

   30819F300D06092A864886F70D010101050003818D0030818902818100BF00CF5B0FC7B9DA
```

```
   6AB174B8F791617F737BD82DE62BA6E08F93067AEAC21AC025307DAF5C2C2934B95AD686C6
   9D6281E76387E938743A29033123456789054FEFC0BE17FDCBA9E470BE1DCB1FF6D8E5B10E
   A3BC17337C52A34297C849B3EF15D08FE49A239A3574516F5EF2C97234B588071A0E89CC7F
   786818BBD277CA84FF0203010001

==============================================
Key name: serverkey(default)
Key type: RSA
Time when key pair created: 17:51:54 2015/03/26
Key code:

   307C300D06092A864886F70D0101010500036B003068026100C9A1E046BBEF0B7CAE47A07C
   DF278BA5B7C0BADC12462EEB1234567890541FFD2935C27F8220AA7AE0DBB1600091E104CA
   F8577E0EAE794EC8BB8E094CEBA16277583A06EF175EC91FE6E0045EFC806B551402940EC9
   4074F97B9588FF45FDFF0203010001
```

Cisco

Note: must configure the hostname and default domain before the 'crypto key generate' process.

```
Cisco(config)#hostname Cisco

Cisco(config)#ip domain-name test


Cisco(config)#crypto ?
  ca   Certification authority
  key  Long term key operations
  pki  Public Key components

Cisco(config)#crypto key ?
  decrypt       Decrypt a keypair.
  encrypt       Encrypt a keypair.
  export        Export keys
  generate      Generate new keys
  import        Import keys
  move          Move keys
  pubkey-chain  Peer public key chain management
  storage       default storage location for keypairs
  zeroize       Remove keys

Cisco(config)#crypto key generate ?
  rsa  Generate RSA keys
  <cr>

Cisco(config)#crypto key generate
The name for the keys will be: Cisco.test
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]


Cisco(config)#ip ssh ?
  authentication-retries  Specify number of authentication retries
  break-string            break-string
  dh                      Diffie-Hellman
  dscp                    IP DSCP value for SSH traffic
  logging                 Configure logging for SSH
  maxstartups             Maximum concurrent sessions allowed
  port                    Starting (or only) Port number to listen on
  precedence              IP Precedence value for SSH traffic
```

```
  pubkey-chain            pubkey-chain
  rsa                     Configure RSA keypair name for SSH
  source-interface        Specify interface for source address in SSH
                          connections
  stricthostkeycheck      Enable SSH Server Authentication
  time-out                Specify SSH time-out interval
  version                 Specify protocol version to be supported

Cisco(config)#ip ssh version ?
  <1-2>  Protocol version

Cisco(config)#ip ssh version 2


Cisco(config)#line vty 0 15

Cisco(config-line)#login ?
  local   Local password checking
  <cr>

Cisco(config-line)#login local ?
  <cr>

Cisco(config-line)#login local

Cisco(config-line)#transport ?
  input      Define which protocols to use when connecting to the terminal
             server
  output     Define which protocols to use for outgoing connections
  preferred  Specify the preferred protocol to use

Cisco(config-line)#transport input ?
  all     All protocols
  none    No protocols
  ssh     TCP/IP SSH protocol
  telnet  TCP/IP Telnet protocol

Cisco(config-line)#transport input ssh ?
  telnet  TCP/IP Telnet protocol
  <cr>

Cisco(config-line)#transport input ssh


Cisco(config)#username <name> privilege 15 password <password>


Cisco#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDEbwH5h57hZcqQbC07QmgIUC7icCexxBtx52vejCnp
ZAsaZzXMXahBSiGYs+GTZePb12345678905Zrk1BwpoZICOO5S8Fk7Gu0e9ilfRdETAstz01YmboasSJ
5rUp3sIasRHGMp3CZHQt520Dv22bDHoCBGEQ8+JF5IJ0kgYkhw==


Cisco#show ssh
Connection Version Mode Encryption  Hmac         State                 Username
0          2.0     IN   aes256-cbc  hmac-sha1    Session started       manager
0          2.0     OUT  aes256-cbc  hmac-sha1    Session started       manager
%No SSHv1 server connections running.
```

```
Cisco#show crypto key mypubkey rsa
% Key pair was generated at: 18:03:26 US-Cent Feb 28 1993
Key name: TP-self-signed-2443920256
 Storage Device: private-config
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00C46F01
  F9879EE1 65CA906C 2D3B4268 08502EE2 7027B1C4 1B71E76B DE8C29E9 640B1A67
  35CC5DA8 414A2198 B3E19365 E312384E 9A386D0D D80699AE 4D41C29A 1920238E
  E52F0593 B1AED1EF 6295F45D 11302CB7 3D356266 E86A4569 E6B529DE C21AB111
  C6329DC2 64742DE7 6D03BF6D 9B0C7A02 046110F3 E245E482 74920624 87020301 0001
% Key pair was generated at: 01:34:01 US-Cent Mar 27 2015
Key name: TP-self-signed-2443920256.server
Temporary key
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00B51791 797FFD80
  F0484B82 1F944989 BF12382B 035B1DC4 92B6C4D9 F9FF1AE8 B8D6CDFF B6AF6BDF
  A9764C7B CB1B9E58 C711892E 1C2B11F5 D1A38AA2 1C456427 2D3F2A49 5757F8D4
  8F9D0DA4 FBD0AD43 CC513CA3 91F790F1 0B57EBC6 2164D46E 85020301 0001
% Key pair was generated at: 02:28:42 US-Cent Mar 27 2015
Key name: Cisco.test
 Storage Device: not specified
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00AB1487 78C90D6E
  3332E08F AD4B26DB 541233F8 1D56986A 5F89DB27 074456AD 07022442 F6DB3765
  4CF3E3FE 7C55A9A7 F958A17C 2CDFCD8B 1E7F86C6 B41894EB 6B020301 0001
```

Chapter 9 GUI Management Access – HTTP and HTTPS

This chapter compares the commands used to enable and configure browser-based applications to manage the switch via unencrypted and encrypted network acess methods.

You can enable standard TCP port 80 access for unencrypted management access to the switch. For encrypted management accesss to the switch via TCP port 443, you must enable and configure Secure Sockets Layer (SSL).

Comware5 notes:

1) Comware5 version 5.20 F2218P01-US and higher support self-signed certificates.
2) HTTP on Comware5 does not support 'authentication-mode password' on vty interfaces and must be configured for 'authentication-mode scheme'.

You can find configuration details for User ID's and Password's in Chapter 2.

a) HTTP

ArubaOS-Switch	Comware5	Cisco
HTTP access is enabled by default and is available as soon as an IP addr is assigned to a VLAN, without UID/PW access control. To control HTTPS access with UID/PW or PW (only), see Ch2 for configuring UID/PW or PW only.	On Comware5, HTTP is not enabled by default, but is enabled once any configuration has been invoked, then requires: 1) configure local uid/pw with 'service-type web' 2) enable http support	HTTP server is enabled by default, but must configure http authentication type. Must have all the device web files for full functionality.
	Comware5 on 3Com "brand" devices has web mgmt enabled by default, use "admin" and no password (if default local user config)	

	`[Comware5]local-user <name>`
	
	`[Comware5-luser-manager]password simple <password>`
	
	`[Comware5-luser-manager]authorization-attribute level 3`
	
	`[Comware5-luser-manager]service-type web`
		`Cisco(config)#username <name> privilege 15 password <password>`

		`Cisco(config)#ip http authentication local`
`ArubaOS-Switch(config)# web-management plaintext`	`[Comware5]ip http enable`	`Cisco(config)#ip http server`
	`[Comware5]display web users`	

	Comware7	
	On Comware7, HTTP is not enabled by default, requires: 1) configure local uid/pw with 'service-type web' 2) enable http support	
	[Comware7]local-user <name> [Comware7-luser-manage-manager]password simple <password> [Comware7-luser-manage-manager]authorization-attribute user-role network-admin [Comware7-luser-manage-manager]service-type http	
	[Comware7]ip http enable	
	[Comware7]display web users	Cisco#show ip http server connection

ArubaOS-Switch

HTTP access is enabled by default and is available as soon as an IP addr is assigned to a VLAN, without UID/PW access control. If passwords are assigned to the operator and/or manager users, then those will be used during HTTP access.

```
ArubaOS-Switch(config)# web-management
 idle-timeout          Set the idle timeout for web management sessions.
 listen                Specify in which mode HTTP Server should listen in
 management-url        Specify URL for web interface [?] button.
 plaintext             Enable/disable the http server (insecure).
 ssl                   Enable/disable the https server (secure).
 support-url           Specify URL for web interface Support page.
 <cr>

ArubaOS-Switch(config)# web-management plaintext
 <cr>

ArubaOS-Switch(config)# web-management plaintext
```

Note, even though the above command can be entered to enable HTTP access, it is the default state and will not appear in the configuration.

Comware5

HTTP is not enabled by default, but is enabled once any configuration has been invoked.

```
[Comware5]local-user manager

[Comware5-luser-manager]password simple password

[Comware5-luser-manager]authorization-attribute level 3
```

```
[Comware5-luser-manager]service-type web


[Comware5]ip ?
  as-path            Specify an as-path
  community-list     Add a community-list entry
  extcommunity-list  Add an extended community-list entry
  forward-broadcast  Enable forwarding directed-broadcast
  host               Add a new IP host name and address to the IP host name
                     table
  http               Hypertext transfer protocol
  https              Config HTTPS server
  ip-prefix          Specify an address prefix list
  ipv6-prefix        Specify an IPv6 address prefix list
  local              Specify local attribute
  redirects          ICMP redirect function
  route-static       Establish a static route
  rpf-route-static   Establish Multicast static route
  source             Source address of packet
  ttl-expires        ICMP TTL-expire function
  unreachables       ICMP unreachable function
  urpf               Unicast reverse path forward function
  vpn-instance       VPN-Instance

[Comware5]ip http ?
  acl     Specify acl filtering
  dscp    Differentiated Services Codepoint (DSCP)
  enable  Start http server
  port    Specify port

[Comware5]ip http enable ?
  <cr>

[Comware5]ip http enable


[Comware5]display web ?
  users  Web management users

[Comware5]display web users ?
  |     Matching output
  <cr>

[Comware5]display web users
UserID    Name       Language  Level      State    LinkCount LoginTime LastTime
ab0c0000  manager    English   Management Enable      0      14:44:45  14:44:51
```

Comware7

HTTP is not enabled by default.

```
[Comware7]local-user manager

[Comware7-luser-manage-manager]password simple password
```

```
[Comware7-luser-manage-manager]authorization-attribute user-role network-admin

[Comware7-luser-manage-manager]service-type http


[Comware7]ip ?
  as-path            Specify an AS path
  community-list     Specify a community list entry
  extcommunity-list  Specify an extended community-list entry
  fast-forwarding    IP fast-forwarding information
  host               Add a static host name-to-IPv4 address mapping
  http               Hypertext Transfer Protocol (HTTP) module
  https              Hypertext Transfer Protocol Secure (HTTPS) module
  icmp               Specify ICMP configuration information
  load-sharing       IP forwarding load-sharing
  local              Apply a policy to locally generated packets
  prefix-list        Specify an IPv4 prefix list
  redirects          Send ICMP Redirect packets
  route-static       Establish a static route
  rpf-route-static   Specify static multicast route
  source             Source binding function
  ttl-expires        Send ICMP Time Exceeded packets
  unreachables       Send ICMP Destination Unreachable packets
  urpf               Unicast reverse path forward function
  vpn-instance       Specify a VPN instance

[Comware7]ip http ?
  acl     Specify a basic IPv4 ACL to filter hosts that use HTTP service
  enable  Enable HTTP server
  port    Specify an HTTP server port number

[Comware7]ip http enable ?
  <cr>


[Comware7]display web ?
  menu   Web menu information
  users  Web users

[Comware7]display web users ?
  >     Redirect it to a file
  >>    Redirect it to a file in append mode
  |     Matching output
  <cr>

[Comware7]display web users
UserID          Name            Type   Language JobCount LoginTime LastOperation
900b01302b0010f manager         HTTP   English     0     15:39:39  15:49:02
```

Cisco

HTTP server is enabled by default, but must configure http authentication type.

Note: must have all the device web files (these are in addition to IOS) on the switch for full functionality.

```
Cisco(config)#username manager privilege 15 password password


Cisco(config)#ip http ?
  access-class                   Restrict http server access by access-class
  active-session-modules         Set up active http server session modules
  authentication                 Set http server authentication method
  client                         Set http client parameters
  help-path                      HTML help root URL
  max-connections                Set maximum number of concurrent http server
                                 connections
  path                           Set base path for HTML
  port                           Set http server port
  secure-active-session-modules  Set up active http secure server session
                                 modules
  secure-ciphersuite             Set http secure server ciphersuite
  secure-client-auth             Set http secure server with client
                                 authentication
  secure-port                    Set http secure server port number for
                                 listening
  secure-server                  Enable HTTP secure server
  secure-trustpoint              Set http secure server certificate trustpoint
  server                         Enable http server
  session-module-list            Set up a http(s) server session module list
  timeout-policy                 Set http server time-out policy parameters

Cisco(config)#ip http authentication ?
  aaa     Use AAA access control methods
  enable  Use enable passwords
  local   Use local username and passwords

Cisco(config)#ip http authentication local ?
  <cr>

Cisco(config)#ip http authentication local


Cisco(config)#ip http server ?
  <cr>

Cisco(config)#ip http server


Cisco#show ip http server connection

HTTP server current connections:
local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes
    10.0.111.41:80         10.1.1.108:55648 1612       70843
```

b) HTTPS - SSL (Self-Signed Certificates)

ArubaOS-Switch	Comware5	Cisco
		`http secure-server` is enabled by default and a self-signed certificate is automatically generated
	[Comware5]local-user <name> [Comware5-luser-manager]password simple <password> [Comware5-luser-manager]authorization-attribute level 3 [Comware5-luser-manager]service-type web	
ArubaOS-Switch(config)# crypto pki enroll-self-signed certificate-name localcert subject		Cisco(config)#crypto key generate rsa
ArubaOS-Switch(config)# web-management ssl	[Comware5]ip https enable	Cisco(config)#ip http secure-server
ArubaOS-Switch(config)# no web-management plaintext	[Comware5]undo ip http enable	Cisco(config)#no ip http server
ArubaOS-Switch# show crypto pki local-certificate ArubaOS-Switch# show crypto pki local-certificate localcert		Cisco#show crypto pki certificates verbose
	[Comware5]display web users	Cisco#show ip http server connection
	Comware7	
	[Comware7]local-user manager [Comware7-luser-manage-manager]password simple password [Comware7-luser-manage-manager]authorization-attribute user-role network-admin [Comware7-luser-manage-manager]service-type https	
	[Comware7]ip https enable	
	[Comware7]undo ip http enable	
	[Comware7]display web users	

ArubaOS-Switch

```
ArubaOS-Switch(config)# crypto ?
 key                    Install/remove RSA key file for ssh.
 pki                    Public Key Infrastructure management

ArubaOS-Switch(config)# crypto pki ?
 clear                  Clears the csr, certificate and its related private key.
 create-csr             Manually create a certificate signing request.
 enroll-self-signed     Create and install a self-signed certificate.
 identity-profile       Creates an identity profile.
 install-signed-cer...  Manually install a signed certificate, the certificatemust match a
                        previously created signing request.
 ta-profile             Creates a Trust Anchor profile.
 zeroize                Remove all pki configuration, including profiles, certificates and
                        keys.

ArubaOS-Switch(config)# crypto pki enroll-self-signed ?
 certificate-name       Name of the local certificate.

ArubaOS-Switch(config)# crypto pki enroll-self-signed certificate-name ?
 CERT-NAME              Name of the local certificate.

ArubaOS-Switch(config)# crypto pki enroll-self-signed certificate-name localcert ?
 key-size               The length of the key, default is 1024 bits.
 subject                Subject fields of the certificate, the default values are
                        specified in the identity profile.
 usage                  The intended application, default is web.
 valid-start            Certificate validity start date (MM/DD/YYYY).
 <cr>

ArubaOS-Switch(config)# crypto pki enroll-self-signed certificate-name localcert subject ?
 common-name            To specify common name
 country                To specify the two letter ISO 3166-1 country code
 locality               To specify locality
 org                    To specify organization
 org-unit               To specify organization unit
 state                  To specify state
 key-size               The length of the key, default is 1024 bits.
 usage                  The intended application, default is web.
 valid-start            Certificate validity start date (MM/DD/YYYY).
 <cr>

ArubaOS-Switch(config)# crypto pki enroll-self-signed certificate-name localcert subject
Enter Common Name(CN) : ArubaOS-Switch
Enter Org Unit(OU) : Lab
Enter Org Name(O) : Test
Enter Locality(L) : Any City
Enter State(ST) : Any State
Enter Country(C) :


ArubaOS-Switch(config)# web-management
 idle-timeout           Set the idle timeout for web management sessions.
 listen                 Specify in which mode HTTP Server should listen in
 management-url         Specify URL for web interface [?] button.
 plaintext              Enable/disable the http server (insecure).
 ssl                    Enable/disable the https server (secure).
 support-url            Specify URL for web interface Support page.
 <cr>
ArubaOS-Switch(config)# web-management ssl
 TCP/UDP-PORT           TCP port on which https server should accept connections.
 <cr>
```

```
ArubaOS-Switch(config)# web-management ssl


ArubaOS-Switch(config)# no web-management plaintext


ArubaOS-Switch# show crypto ?
 autorun-cert          Display trusted certificate.
 autorun-key           Display autorun key.
 client-public-key     Display ssh authorized client public keys.
 host-public-key       Display ssh host RSA public key.
 pki                   Displays the PKI related information.

ArubaOS-Switch# show crypto pki ?
 identity-profile      Show the configured switch identity.
 local-certificate     Show local certificate information.
 ta-profile            Show Trust Anchor profile specific details.

ArubaOS-Switch# show crypto pki local-certificate ?
 CERT-NAME             Enter the Certificate name to get the details
 summary               Displays the summary of all the certificates in the switch
 <cr>

ArubaOS-Switch# show crypto pki local-certificate
   Name                 Usage      Expiration     Parent / Profile
   -------------------- ---------- -------------- --------------------
   localcert            Web        2016/03/27     default

ArubaOS-Switch# show crypto pki local-certificate localcert
Certificate Detail:
Version: 3 (0x2)
Serial Number:
   32:ef:31:80:90:17:da:5a:f2:da:b4:42:96:b9:57:40:57:4e:99:77
Signature Algorithm: sha256withRSAEncryption
Issuer: CN=ArubaOS-Switch, OU=Lab, O=Test, L=Any City, ST=Any State, C=US
Validity
   Not Before: Mar 27 17:22:13 2015 GMT
   Not After : Mar 27 23:59:59 2016 GMT
Subject: CN=ArubaOS-Switch, OU=Lab, O=Test, L=Any City, ST=Any State, C=US
Subject Public Key Info:
   Public Key Algorithm: rsaEncryption
   RSA Public Key: (1024 bit)
      Modulus (1024 bit):
          bb:35:e9:41:ec:ad:80:d9:3d:95:21:8a:48:77:63:
          93:7f:73:99:60:5e:0f:73:1f:9d:86:b5:6b:19:d9:
          40:e2:b5:fd:6f:0f:74:89:60:40:59:91:2c:71:f3:
          1c:5d:6b:e0:f6:d7:a6:64:7f:8a:02:57:ff:be:a9:
          1d:59:4b:e9:41:49:ba:bc:e1:ff:35:00:c0:09:a7:
          c5:e9:9d:59:05:bd:2f:1e:32:62:76:eb:95:5b:40:
          42:8a:61:7c:05:0b:f2:d0:ad:66:0b:0e:e2:94:8a:
          71:ce:31:00:bd:cd:cb:84:80:03:47:b7:43:88:2e:
          f7:d3:de:39:b9:c3:15:c5
      Exponent: 65537 (0x10001)
X509v3 extensions:
   X509v3 Key Usage: critical
      Digital Signature, Key Encipherment, Key Agreement,
      Decipher Only
   X509v3 Extended Key Usage:
      TLS Web Server Authentication

Signature Algorithm: sha256withRSAEncryption
   3e:c2:63:05:b0:e0:2c:a3:50:f9:7c:3e:a5:39:92:3d:d3:47:
   4a:bd:57:8c:80:33:e6:e2:bc:0f:bd:73:68:83:e4:a0:5f:04:
```

```
   20:71:26:fa:c7:c0:2a:26:a1:00:76:7b:46:f6:9f:43:96:94:
   e5:44:23:b9:38:85:bb:0d:64:8c:18:f0:0f:25:83:b3:99:30:
   33:e0:5e:f3:50:53:15:01:74:dc:41:f8:4d:5d:bc:1e:4d:a1:
   c3:a1:e9:6a:47:70:d5:39:42:69:38:02:9f:be:a7:05:a9:01:
   77:cc:05:6e:56:07:f8:7c:bb:e8:28:6b:be:bf:3b:4a:73:f3:
   87:c3
MD5 Fingerprint: c361 035b a941 cb31 334e c383 0a2b 7526
SHA1 Fingerprint: f6b0 eefb 57b8 ba32 6efa cc56 9f2d 8053 4ed3 e692
```

Comware5

```
[Comware5]local-user manager

[Comware5-luser-manager]password simple password

[Comware5-luser-manager]authorization-attribute level 3

[Comware5-luser-manager]service-type web


[Comware5]ip http?
   http
   https

[Comware5]ip https ?
  acl                Specify acl filtering
  certificate        Specify certificate access-control-policy of HTTPS server
  enable             Start HTTPS server
  port               Specify port
  ssl-server-policy  Specify SSL server policy of HTTPS server

[Comware5]ip https enable ?
  <cr>

[Comware5]ip https enable


[Comware5]undo ip http enable


[Comware5]display web users
UserID    Name       Language  Level      State    LinkCount LoginTime LastTime
ab140000  manager    English   Management Enable      0      17:38:02  17:38:14
```

Comware7

```
[Comware7]local-user manager

[Comware7-luser-manage-manager]password simple password

[Comware7-luser-manage-manager]authorization-attribute user-role network-admin

[Comware7-luser-manage-manager]service-type https


[Comware]ip http?
   http
   https

[Comware7]ip http?
  http
  https

[Comware7]ip https ?
  acl                Specify a basic IPv4 ACL to filter hosts that use HTTPS
                     service
```

```
  certificate        Specify certificate-based identity authentication
  enable             Enable HTTPS server
  port               Specify an HTTPS server port number
  ssl-server-policy  Specify an SSL server policy for HTTPS access control

[Comware7]ip https enable ?
  <cr>

[Comware7]ip https enable
The system might take several minutes to enable the HTTPS service. Please wait...

[Comware7]undo ip http enable


[Comware7]display web users
UserID          Name            Type   Language JobCount LoginTime LastOperation
100b05f02c00100 manager         HTTPS  English     0     17:46:13  17:46:28
```

Cisco

Note: http secure-server is enabled by default and a self-signed certificate is automatically generated.

Note: if a default domain has not been configured, configure before the 'crypto key generate' process.

Note: must have all the web files on the switch for full functionality.

```
Cisco(config)#crypto ?
  ca   Certification authority
  key  Long term key operations
  pki  Public Key components

Cisco(config)#crypto key ?
  decrypt       Decrypt a keypair.
  encrypt       Encrypt a keypair.
  export        Export keys
  generate      Generate new keys
  import        Import keys
  move          Move keys
  pubkey-chain  Peer public key chain management
  storage       default storage location for keypairs
  zeroize       Remove keys

Cisco(config)#crypto key generate ?
  rsa  Generate RSA keys
  <cr>

Cisco(config)#crypto key generate rsa ?
  encryption    Generate a general purpose RSA key pair for signing and
                encryption
  exportable    Allow the key to be exported
  general-keys  Generate a general purpose RSA key pair for signing and
                encryption
  label         Provide a label
  modulus       Provide number of modulus bits on the command line
  on            create key on specified device.
  redundancy    Allow the key to be synced to high-availability peer
  signature     Generate a general purpose RSA key pair for signing and
                encryption
  storage       Store key on specified device
  usage-keys    Generate separate RSA key pairs for signing and encryption
  <cr>
```

```
Cisco(config)#crypto key generate rsa
The name for the keys will be: Cisco.text
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...
[OK]


Cisco(config)#ip http ?
  access-class                   Restrict http server access by access-class
  active-session-modules         Set up active http server session modules
  authentication                 Set http server authentication method
  client                         Set http client parameters
  help-path                      HTML help root URL
  max-connections                Set maximum number of concurrent http server
                                 connections
  path                           Set base path for HTML
  port                           Set http server port
  secure-active-session-modules  Set up active http secure server session
                                 modules
  secure-ciphersuite             Set http secure server ciphersuite
  secure-client-auth             Set http secure server with client
                                 authentication
  secure-port                    Set http secure server port number for
                                 listening
  secure-server                  Enable HTTP secure server
  secure-trustpoint              Set http secure server certificate trustpoint
  server                         Enable http server
  session-module-list            Set up a http(s) server session module list
  timeout-policy                 Set http server time-out policy parameters

Cisco(config)#ip http secure-server ?
  <cr>

Cisco(config)#ip http secure-server
```

Note: `ip http secure-server` is enabled by default and a self-signed certificate is automatically generated.

```
Cisco(config)#no ip http server


Cisco#show crypto ?
  key  Show long term public keys
  pki  Show PKI

Cisco#show crypto pki certificates ?
  WORD     Trustpoint Name
  storage  show certificate storage location
  verbose  Display in verbose mode
  |        Output modifiers
  <cr>

Cisco#show crypto pki certificates verbose
Router Self-Signed Certificate
  Status: Available
```

```
  Version: 3
  Certificate Serial Number (hex): 01
  Certificate Usage: General Purpose
  Issuer:
    cn=IOS-Self-Signed-Certificate-2443680256
  Subject:
    Name: IOS-Self-Signed-Certificate-2443943256
    cn=IOS-Self-Signed-Certificate-2443920256
  Validity Date:
    start date: 18:05:27 US-Cent Feb 28 1993
    end   date: 18:00:00 US-Cent Dec 31 2019
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
  Signature Algorithm: MD5 with RSA Encryption
  Fingerprint MD5: DFDE78DB F9836CBF 9034F31F AC631A7B
  Fingerprint SHA1: E075DAB4 B34456097 6BCF3470 2249CD92 CE795CC4
  X509v3 extensions:
    X509v3 Subject Key ID: 2A08544F 345B765D EA8BCB28 4E0A2AFD 0F73E9CD
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Subject Alternative Name:
        Cisco.test
    X509v3 Authority Key ID: 2A08544F 3371265D EA8BCB28 4E0A2AFD 0F73E9CD
    Authority Info Access:
  Associated Trustpoints: TP-self-signed-2443920256
  Storage: nvram:IOS-Self-Sig#3.cer


Cisco#show ip http server connection

HTTP server current connections:
local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes
    10.0.111.41:443        10.1.1.108:55952 1997       58595
```

Chapter 10 RADIUS Authentication for Switch Management

This chapter covers the commands required to authenticate management users to a network Remote Authentication Dial-In User Service (RADIUS) server.

RADIUS is a distributed information interaction protocol that uses a client/server model. It provides access authentication and authorization services and is often used in network environments requiring both high security and remote user access. Originally designed for dial-in user access, it now supports additional access methods, such as Ethernet and Asymmetric Digital Subscriber Line (ADSL).

Running on the switch, the RADIUS client passes user information to designated RADIUS servers and acts on the responses (for example, rejecting or accepting user access requests).

RADIUS is described in RFC 2865 for Authentication and Authorization, and in RFC 2866 for Accounting. The RADIUS accounting function collects and records network resource usage information.

RADIUS uses UDP as the transport protocol. It uses UDP port 1812 for authentication and UDP port 1813 for accounting.

Huawei Terminal Access Controller Access Control System (HWTACACS) also provides authentication, authorization, and accounting services. RADIUS and HWTACACS have many features in common, including a client/server model, the use of shared keys for user information security, and flexibility and extensibility. Their differences are listed in the following table:

RADIUS	HWTACACS
RADIUS uses UDP, providing higher transport efficiency.	HWTACACS uses TCP, providing more reliable network transmission.
It encrypts only the user password field in an authentication packet.	It encrypts the entire packet, except for the HWTACACS header.
Protocol packets are simple and the authorization process is combined with the authentication process.	Protocol packets are complicated and authorization is independent of authentication. You can deploy authentication and authorization on different HWTACACS servers.
RADIUS does not support authorization of configuration commands. A user can use all the commands at our below the user's level. (ArubaOS-Switch has this as a feature using VSA configuration parameters on the RADIUS server that are passed to the NAS.)	HWTACACS supports authorization of configuration commands. A user can use commands that are at or below the user's level or are authorized by the HWTACACS server.

a) Basic Configuration

ArubaOS-Switch	Comware5	Cisco
	(If you are planning to use Telnet or SSH, you should configure those features before you configure AAA support.) (See notes below concerning login procedures for RADIUS.)	
	`[Comware5]radius scheme radius-auth`	`Cisco(config)#radius server radius-auth`

`ArubaOS-Switch(config)# radius-server host 10.0.100.111 key password`	`[Comware5-radius-radius-auth]primary authentication 10.0.100.111 key simple password`
	
	`[Comware5-radius-radius-auth]primary accounting 10.0.100.111 key simple password`
	
	`[Comware5-radius-radius-auth]user-name-format without-domain`
	
	`[Comware5-radius-radius-auth]server-type extended`
		`Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key password`

`ArubaOS-Switch(config)#radius-server host <IP-ADDR> time-window <Seconds>`		`Cisco(config)#radius-server dead-criteria time <time > <tries >`
`ArubaOS-Switch(config)#radius-server host <IP-ADDR> time-window positive-time-window`		`Cisco(config)#radius -server deadtime minutes`
`ArubaOS-Switch(config)#radius-server host <IP-ADDR> time-window plus-or-minus-time-window`		`Cisco(config)#radius -server host ip-address [ acct-port udp-port ] [ auth-port udp-port ] [ test username name [ idle-time time ] [ ignore-acct-port ] [ ignore-auth-port ]] [ key string ]`
`ArubaOS-Switch(config)# aaa authentication console login radius local`		`Cisco(config)#aaa authentication login default group radius local`
`ArubaOS-Switch(config)# aaa authentication console enable radius local`		`Cisco(config)#aaa authentication enable default group radius local`
`ArubaOS-Switch(config)# aaa authentication telnet login radius none`		`Cisco(config)#aaa authentication login default group radius`
`ArubaOS-Switch(config)# aaa authentication telnet enable radius none`		`Cisco(config)#aaa authentication enable default group radius`

ArubaOS-Switch(config)# aaa authentication ssh login radius none		Cisco(config)#aaa authentication login default group radius
ArubaOS-Switch(config)# aaa authentication ssh enable radius none		Cisco(config)#aaa authentication enable default group radius
ArubaOS-Switch(config)# aaa authentication web login radius none		
ArubaOS-Switch(config)# aaa authentication web enable radius none		
	[Comware5]domain lab [Comware5-isp-lab]authentication default radius-scheme radius-auth [Comware5-isp-lab]authorization default radius-scheme radius-auth [Comware5-isp-lab]accounting default radius-scheme radius-auth	
	[Comware5]domain default enable lab	
	[Comware5]user-interface aux 0	
	[Comware5-ui-aux0]authentication-mode scheme	
	[Comware5]user-interface vty 0 15	Cisco(config)#line vty 0 15
	[Comware5-ui-vty0-15]authentication-mode scheme [Comware5-ui-vty0-15]user privilege level 3	Cisco(config-line)#login authentication default
ArubaOS-Switch# show radius	[Comware5]display radius scheme	Cisco#show aaa servers Cisco#show radius server-group radius
ArubaOS-Switch# show authentication		
ArubaOS-Switch# show radius authentication		
ArubaOS-Switch# show radius host 10.0.100.111	[Comware5]display radius statistics	Cisco#show radius statistics
	Comware7	
	(If you are planning to use Telnet or SSH, you should configure those features before you configure AAA support.) (See notes below concerning login procedures for RADIUS.)	

	[Comware7]radius scheme radius-auth	
	[Comware7-radius-radius-auth]primary authentication 10.0.100.111 key simple password [Comware7-radius-radius-auth]primary accounting 10.0.100.111 key simple password [Comware7-radius-radius-auth]user-name-format without-domain	
	[Comware7]domain lab [Comware7-isp-lab]authentication default radius-scheme radius-auth [Comware7-isp-lab]authorization default radius-scheme radius-auth [Comware7-isp-lab]accounting default radius-scheme radius-auth	
	[Comware7]domain default enable lab	
	[Comware7]user-interface aux 0	
	[Comware7-line-aux0]authentication-mode scheme	
	[Comware7]user-interface vty 0 63	
	[Comware7-ui-vty0-63]authentication-mode scheme [Comware7-line-vty0-63]user-role network-admin	
	[Comware7]display radius scheme	
	[Comware7]display radius statistics	

ArubaOS-Switch

```
ArubaOS-Switch(config)# radius-server ?
dead-time              Server unavailability time (default is 0, use the 'no' form of
                        command to set the dead-time to 0).
 dyn-autz-port          UDP port number to listen for Change-of-Authorization and
                        Disconnect messages (default is 3799).
 host                   IPv4/IPv6 address of the RADIUS server to use.
 key                    Global encryption key (default is NULL). If in enhanced
                        secure-mode, you will be prompted for the key.
```

```
 retransmit             Number of packet retransmits (default is 3).
 timeout                Server timeout interval (default is 5).

ArubaOS-Switch(config)# radius-server host
 IPV6-ADDR              IPv6 address of the RADIUS server to use.
 IP-ADDR                IPv4 address of the RADIUS server to use.

ArubaOS-Switch(config)# radius-server host 10.0.100.111
 acct-port              Accounting UDP destination port number(1-65535).
 auth-port              Authentication UDP destination port number (default is 1812).
 dyn-authorization      Enable/disable dynamic authorization control from this host.
 key                    Encryption key to use with the RADIUS server (default is NULL). If
                        in enhanced secure-mode, you will be prompted for the key.
 oobm                   Use OOBM interface to connect to server
 time-window            time window (in seconds) within which the received dynamic
                        authorization requests are considered to be current and accepted
                        for processing.
 <cr>

ArubaOS-Switch(config)# radius-server host 10.0.100.111 key ?
 KEY                    Encryption key to use with the RADIUS server (default is NULL).
 oobm                   Use OOBM interface to connect to server

ArubaOS-Switch(config)# radius-server host 10.0.100.111 key password ?
 acct-port              Accounting UDP destination port number(1-65535).
 auth-port              Authentication UDP destination port number (default is 1812).
 oobm                   Use OOBM interface to connect to server
 <cr>

ArubaOS-Switch(config)# radius-server host 10.0.100.111 key password


ArubaOS-Switch(config)# aaa
 accounting             Configure accounting parameters on the switch.
 authentication         Configure authentication parameters on the switch.
 authorization          Configure authorization parameters on the switch.
 port-access            Configure 802.1X (Port Based Network Access), MAC address based
                        network access, or web authentication based network access on the
                        device.
 server-group           Place the RADIUS server into the RADIUS server group.

ArubaOS-Switch(config)# aaa authentication ?
allow-vlan             Configure authenticator ports to apply VLAN changes immediately.
 console                Configure authentication mechanism used to control access to the
                        switch console.
 disable-username       Bypass the username during authentication while accessing the
                        switch to get Manager or Operator access.
 local-user             Create or remove a local user account.
 lockout-delay          The number of seconds after repeated login failures before a user
                        may again attempt login.
 login                  Specify that switch respects the authentication server's privilege
                        level.
 mac-based              Configure authentication mechanism used to control mac-based port
                        access to the switch.
 num-attempts           The number of login attempts allowed.
 port-access            Configure authentication mechanism used to control access to the
                        network.
 ssh                    Configure authentication mechanism used to control SSH access to
                        the switch.
 telnet                 Configure authentication mechanism used to control telnet access
                        to the switch.
 web                    Configure authentication mechanism used to control web access to
                        the switch.
```

```
 web-based             Configure authentication mechanism used to control web-based port
                       access to the switch.

ArubaOS-Switch(config)# aaa authentication console ?
 enable                Configure access to the privileged mode commands.
 login                 Configure login access to the switch.

ArubaOS-Switch(config)# aaa authentication console login ?
 local                 Use local switch user/password database.
 tacacs                Use TACACS+ server.
 radius                Use RADIUS server.
 peap-mschapv2         Use RADIUS server with PEAP-MSChapv2.

ArubaOS-Switch(config)# aaa authentication console login radius ?
 local                 Use local switch user/password database.
 none                  Do not use backup authentication methods.
 authorized            Allow access without authentication.
 server-group          Specify the server group to use.
 <cr>

ArubaOS-Switch(config)# aaa authentication console login radius local ?
 <cr>

ArubaOS-Switch(config)# aaa authentication console login radius local


ArubaOS-Switch(config)# aaa authentication console enable radius local


ArubaOS-Switch(config)# aaa authentication telnet login radius none


ArubaOS-Switch(config)# aaa authentication telnet enable radius none


ArubaOS-Switch(config)# aaa authentication ssh login radius none


ArubaOS-Switch(config)# aaa authentication ssh enable radius none

ArubaOS-Switch(config)# aaa authentication web login radius none

ArubaOS-Switch(config)# aaa authentication web enable radius none


ArubaOS-Switch# show radius

 Status and Counters - General RADIUS Information

  Deadtime (minutes)             : 0
  Timeout (seconds)              : 5
  Retransmit Attempts            : 3
  Global Encryption Key          :
  Dynamic Authorization UDP Port : 3799
  Source IP Selection            : 10.0.111.21

                  Auth Acct DM/ Time   |
  Server IP Addr  Port Port CoA Window | Encryption Key                    OOBM
  --------------- ---- ---- --- ------ + -------------------------------- ----
  10.0.100.111    1812 1813 No  300    | password                         No


ArubaOS-Switch# show authentication
```

```
 Status and Counters - Authentication Information

  Login Attempts : 3
  Lockout Delay : 0
  Respect Privilege : Disabled
  Bypass Username For Operator and Manager Access : Disabled

                  | Login      Login        Login
  Access Task     | Primary    Server Group Secondary
  -------------- + ---------- ------------ ----------
  Console         | Radius     radius       Local
  Telnet          | Radius     radius       None
  Port-Access     | Local                   None
  Webui           | Radius     radius       None
  SSH             | Radius     radius       None
  Web-Auth        | ChapRadius radius       None
  MAC-Auth        | ChapRadius radius       None
  SNMP            | Local                   None
  Local-MAC-Auth  | Local      radius       None
                  | Local                   None

                  | Enable     Enable       Enable
  Access Task     | Primary    Server Group Secondary
  -------------- + ---------- ------------ ----------
  Console         | Radius     radius       Local
  Telnet          | Radius     radius       None
  Webui           | Radius     radius       None
  SSH             | Radius     radius       None

ArubaOS-Switch# show radius authentication

 Status and Counters - RADIUS Authentication Information

  NAS Identifier           : ArubaOS-Switch
  Invalid Server Addresses : 0
                   UDP
  Server IP Addr  Port Timeouts   Requests   Challenges Accepts    Rejects
  --------------- ---- ---------- ---------- ---------- ---------- ----------
  10.0.100.111    1812 0          6          0          5          1

ArubaOS-Switch# show radius host 10.0.100.111

 Status and Counters - RADIUS Server Information


  Server IP Addr : 10.0.100.111

  Authentication UDP Port : 1812         Accounting UDP Port  : 1813
  Round Trip Time         : 0            Round Trip Time      : 0
  Pending Requests        : 0            Pending Requests     : 0
  Retransmissions         : 0            Retransmissions      : 0
  Timeouts                : 0            Timeouts             : 0
  Malformed Responses     : 0            Malformed Responses  : 0
  Bad Authenticators      : 0            Bad Authenticators   : 0
  Unknown Types           : 0            Unknown Types        : 0
  Packets Dropped         : 0            Packets Dropped      : 0
  Access Requests         : 6            Accounting Requests  : 0
  Access Challenges       : 0            Accounting Responses : 0
  Access Accepts          : 5
  Access Rejects          : 1
```

Comware5

(If you are planning to use Telnet or SSH, you should configure those features before you configure AAA support.)

Special note on using AAA authentication. By default Comware5 is expecting a user to login as "user@domain", this allows for multiple domain support.

In order to support a user to supply only their UID without the "@domain", the '`user-name-format without-domain`' parameter can be configured within the radius scheme, which allows Comware5 to send just a UID to the RADIUS server.

```
[Comware5]radius ?
  client         Radius Client config
  dscp           Set DSCP (DiffServ CodePoints) value of RADIUS packets
  ipv6           Specify IPv6 configuration
  nas-backup-ip  Specify RADIUS client backup IP address
  nas-ip         Specify RADIUS client IP address
  scheme         Add RADIUS scheme or modify radius-scheme attributes
  trap           Specify trap configuration

[Comware5]radius scheme ?
  STRING<1-32>  Radius scheme name

[Comware5]radius scheme radius-auth
New Radius scheme

[Comware5-radius-radius-auth]?
Radius-template view commands:
  accounting-on           Accounting-On packet sending mode
  attribute               Customize selected RADIUS attributes
  cfd                     Connectivity fault detection (IEEE 802.1ag)
  data-flow-format        Specify data flow format
  display                 Display current system information
  key                     Specify the shared encryption key of RADIUS server
  mtracert                Trace route to multicast source
  nas-backup-ip           Specify RADIUS client backup IP address
  nas-ip                  Specify RADIUS client IP address
  ping                    Ping function
  primary                 Specify IP address of primary RADIUS server
  quit                    Exit from current command view
  retry                   Specify retransmission times
  return                  Exit to User View
  save                    Save current configuration
  secondary               Specify IP address of secondary RADIUS server
  security-policy-server  Specify IP address of security policy server
  server-type             Specify the type of RADIUS server
  state                   Specify state of primary/secondary
                          authentication/accounting RADIUS server
  stop-accounting-buffer  Enable stop-accounting packet buffer
  timer                   Specify timer parameters
  tracert                 Trace route function
  undo                    Cancel current setting
  user-name-format        Specify user-name format sent to RADIUS server
  vpn-instance            Specify VPN instance

[Comware5-radius-radius-auth]primary ?
  accounting      Specify IP address of primary accounting RADIUS server
  authentication  Specify IP address of primary authentication RADIUS server

[Comware5-radius-radius-auth]primary authentication ?
```

```
  X.X.X.X  Any valid IP address
  ipv6     Specify IPV6 address

[Comware5-radius-radius-auth]primary authentication 10.0.100.111 ?
  INTEGER<1-65535>  Authentication-port : generally is 1812
  key               Specify the shared encryption key of RADIUS server
  probe             Probe the server to determine its availability
  vpn-instance      Specify VPN instance
  <cr>

[Comware5-radius-radius-auth]primary authentication 10.0.100.111 key ?
  STRING<1-64>  Plaintext key string
  cipher        Specify a ciphertext key
  simple        Specify a plaintext key

[Comware5-radius-radius-auth]primary authentication 10.0.100.111 key simple ?
  STRING<1-64>  Plaintext key string

[Comware5-radius-radius-auth]primary authentication 10.0.100.111 key simple password ?
  INTEGER<1-65535>  Authentication-port : generally is 1812
  probe             Probe the server to determine its availability
  vpn-instance      Specify VPN instance
  <cr>

[Comware5-radius-radius-auth]primary authentication 10.0.100.111 key simple password


[Comware5-radius-radius-auth]primary accounting ?
  X.X.X.X  Any valid IP address
  ipv6     Specify IPV6 address

[Comware5-radius-radius-auth]primary accounting 10.0.100.111 ?
  INTEGER<1-65535>  Accounting-port : generally is 1813
  key               Specify the shared encryption key of RADIUS server
  vpn-instance      Specify VPN instance
  <cr>

[Comware5-radius-radius-auth]primary accounting 10.0.100.111 key ?
  STRING<1-64>  Plaintext key string
  cipher        Specify a ciphertext key
  simple        Specify a plaintext key

[Comware5-radius-radius-auth]primary accounting 10.0.100.111 key simple ?
  STRING<1-64>  Plaintext key string

[Comware5-radius-radius-auth]primary accounting 10.0.100.111 key simple password ?
  INTEGER<1-65535>  Accounting-port : generally is 1813
  vpn-instance      Specify VPN instance
  <cr>

[Comware5-radius-radius-auth]primary accounting 10.0.100.111 key simple password


[Comware5-radius-radius-auth]user-name-format ?
  keep-original   User name unchanged
  with-domain     Include the domain name in the username, such as XXX@YYY
  without-domain  Exclude the domain name from the username

[Comware5-radius-radius-auth]user-name-format without-domain ?
  <cr>

[Comware5-radius-radius-auth]user-name-format without-domain
```

```
[Comware5-radius-radius-auth]server-type ?
  extended  Server based on RADIUS extensions
  standard  Server based on RFC protocol(s)

[Comware5-radius-radius-auth]server-type extended ?
  <cr>

[Comware5-radius-radius-auth]server-type extended


[Comware5]domain lab
New Domain added.

[Comware5-isp-lab]?
Isp view commands:

  access-limit              Specify access limit of domain
  accounting                Specify accounting scheme
  authentication            Specify authentication scheme
  authorization             Specify authorization scheme
  authorization-attribute   Specify authorization attributes of domain
  cfd                       Connectivity fault detection (IEEE 802.1ag)
  display                   Display current system information
  dscp                      Specify a DSCP value for user packets of this domain
  idle-cut                  Specify idle-cut attribute of domain
  mtracert                  Trace route to multicast source
  ping                      Ping function
  quit                      Exit from current command view
  return                    Exit to User View
  save                      Save current configuration
  self-service-url          Specify self-service URL(Uniform Resource Locator)
                            of domain
  state                     Specify state of domain
  tracert                   Trace route function
  undo                      Cancel current setting

[Comware5-isp-lab]authentication ?
  default     Specify default AAA configuration
  lan-access  Specify lan-access AAA configuration
  login       Specify login AAA configuration
  portal      Specify portal AAA configuration
  super       Specify super AAA configuration

[Comware5-isp-lab]authentication default ?
  hwtacacs-scheme  Specify HWTACACS scheme
  local            Specify local scheme
  none             Specify none scheme
  radius-scheme    Specify RADIUS scheme

[Comware5-isp-lab]authentication default radius-scheme ?
  STRING<1-32>  Scheme name

[Comware5-isp-lab]authentication default radius-scheme radius-auth

[Comware5-isp-lab]authorization default radius-scheme radius-auth

[Comware5-isp-lab]accounting default radius-scheme radius-auth

[Comware5]domain default enable lab


[Comware5]user-interface aux 0
```

```
[Comware5-ui-aux0]authentication-mode ?
  none      Login without checking
  password  Authentication use password of user terminal interface
  scheme    Authentication use AAA

[Comware5-ui-aux0]authentication-mode scheme ?
  <cr>

[Comware5-ui-aux0]authentication-mode scheme


[Comware5]user-interface vty 0 15

[Comware5-ui-vty0-15]authentication-mode ?
  none      Login without checking
  password  Authentication use password of user terminal interface
  scheme    Authentication use AAA

[Comware5-ui-vty0-15]authentication-mode scheme ?
  <cr>

[Comware5-ui-vty0-15]authentication-mode scheme


[Comware5-ui-vty0-15]user ?
  privilege  Specify the login priority of user terminal interface

[Comware5-ui-vty0-15]user privilege ?
  level  Specify the privilege level of user interface

[Comware5-ui-vty0-15]user privilege level ?
  INTEGER<0-3>  Specify privilege level

[Comware5-ui-vty0-15]user privilege level 3 ?
  <cr>

[Comware5-ui-vty0-15]user privilege level 3


[Comware5]display radius ?
  scheme      The RADIUS scheme information
  statistics  Statistics information

[Comware5]display radius scheme ?
  STRING<1-32>  The RADIUS scheme name in the system. If not inputted, show the
                information of all the RADIUS scheme(s)
  slot          Specify slot number
  |             Matching output
  <cr>

[Comware5]display radius scheme radius-auth
-------------------------------------------------------------------
SchemeName  : radius-auth
  Index : 0                           Type : extended
  Primary Auth Server:
    IP: 10.0.100.111                              Port: 1812   State: active
    Encryption Key : ******
    VPN instance   : N/A
    Probe username : N/A
    Probe interval : N/A
  Primary Acct Server:
    IP: 10.0.100.111                              Port: 1813   State: active
```

```
    Encryption Key : ******
    VPN instance   : N/A
  Auth Server Encryption Key : N/A
  Acct Server Encryption Key : N/A
  VPN instance               : N/A
  Accounting-On packet disable, send times : 50 , interval : 3s
  Interval for timeout(second)                            : 3
  Retransmission times for timeout                        : 3
  Interval for realtime accounting(minute)                : 12
  Retransmission times of realtime-accounting packet      : 5
  Retransmission times of stop-accounting packet          : 500
  Quiet-interval(min)                                     : 5
  Username format                                         : with-domain
  Data flow unit                                          : Byte
  Packet unit                                             : one


-------------------------------------------------------------------
Total 1 RADIUS scheme(s).

[Comware5]display radius statistics ?
  slot  Specify slot number
  <cr>

[Comware5]display radius statistics
Slot  1:state statistic(total=4096):
     DEAD = 4093     AuthProc = 0        AuthSucc = 0
AcctStart = 0         RLTSend = 0         RLTWait = 3
 AcctStop = 0          OnLine = 3            Stop = 0
 StateErr = 0

Received and Sent packets statistic:
Sent PKT total   = 8
Received PKT total = 8
Resend Times     Resend total
Total            0
RADIUS received packets statistic:
Code =  2   Num = 3        Err = 0
Code =  3   Num = 2        Err = 0
Code =  5   Num = 3        Err = 0
Code = 11   Num = 0        Err = 0

Running statistic:
RADIUS received messages statistic:
Auth request             Num = 5        Err = 0        Succ = 5
Account request          Num = 3        Err = 0        Succ = 3
Account off request      Num = 0        Err = 0        Succ = 0
PKT auth timeout         Num = 0        Err = 0        Succ = 0
PKT acct_timeout         Num = 0        Err = 0        Succ = 0
Realtime Account timer   Num = 0        Err = 0        Succ = 0
PKT response             Num = 8        Err = 0        Succ = 8
Session ctrl pkt         Num = 0        Err = 0        Succ = 0
Normal author request    Num = 0        Err = 0        Succ = 0
Set policy result        Num = 0        Err = 0        Succ = 0
Accounting on request    Num = 1        Err = 0        Succ = 1
Accounting on response   Num = 0        Err = 0        Succ = 0
Distribute request       Num = 0        Err = 0        Succ = 0
RADIUS sent messages statistic:
Auth accept              Num = 3
Auth reject              Num = 2
Auth continue            Num = 0
Account success          Num = 3
Account failure          Num = 0
```

```
Server ctrl req           Num = 0
RecError_MSG_sum      = 0
SndMSG_Fail_sum       = 0
Timer_Err             = 0
Alloc_Mem_Err         = 0
State Mismatch        = 0
Other_Error           = 0

No-response-acct-stop packet = 0
Discarded No-response-acct-stop packet for buffer overflow = 0
```

Comware7

(If you are planning to use Telnet or SSH, you should configure those features before you configure AAA support.)

Special note on using AAA authentication. By default Comware7 is expecting a user to login as "user@domain", this allows for multiple domain support.

In order to support a user to supply only their UID without the "@domain", the '`user-name-format without-domain`' parameter can be configured within the radius scheme, which allows Comware7 to send just a UID to the RADIUS server.

```
[Comware7]radius ?
  nas-ip           Specify the RADIUS client IP address
  scheme           Specify RADIUS scheme
  session-control  RADIUS session control function

[Comware7]radius scheme ?
  STRING<1-32>  Radius scheme name

[Comware7]radius scheme radius-auth
New Radius scheme

[Comware7-radius-radius-auth]?
Radius protocol view commands:
  accounting-on           Specify accounting-On function
  attribute               Customize RADIUS attributes
  cfd                     Connectivity Fault Detection (CFD) module
  data-flow-format        Specify the data unit
  diagnostic-logfile      Diagnostic log file configuration
  display                 Display current system information
  key                     Specify a key for secure RADIUS communication
  logfile                 Log file configuration
  monitor                 System monitor
  nas-ip                  Specify the RADIUS client IP address
  ping                    Ping function
  primary                 Specify a primary RADIUS server
  quit                    Exit from current command view
  retry                   Specify retransmission times
  return                  Exit to User View
  save                    Save current configuration
  secondary               Specify a secondary RADIUS server
  security-logfile        Security log file configuration
  security-policy-server  Specify a security policy server
  state                   Specify state of RADIUS server
  timer                   Specify timer parameters
  tracert                 Tracert function
  undo                    Cancel current setting
  user-name-format        Specify user-name format sent to RADIUS server
  vpn-instance            Specify a VPN instance
```

```
[Comware7-radius-radius-auth]primary ?
  accounting      Specify the primary RADIUS accounting server
  authentication  Specify the primary RADIUS authentication server

[Comware7-radius-radius-auth]primary authentication ?
  STRING<1-253>  Host name
  X.X.X.X        IP address
  ipv6           Specify an IPv6 address

[Comware7-radius-radius-auth]primary authentication 10.0.100.111 ?
  INTEGER<1-65535>  Authentication port number, generally is 1812
  key               Specify the shared key for secure communication with the
                    server
  vpn-instance      Specify a VPN instance
  <cr>

[Comware7-radius-radius-auth]primary authentication 10.0.100.111 key ?
  cipher  Specify a ciphertext key
  simple  Specify a plaintext key

[Comware7-radius-radius-auth]primary authentication 10.0.100.111 key simple ?
  STRING<1-64>  Plaintext key string

[Comware7-radius-radius-auth]primary authentication 10.0.100.111 key simple password ?
  INTEGER<1-65535>  Authentication port number, generally is 1812
  vpn-instance      Specify a VPN instance
  <cr>

[Comware7-radius-radius-auth]primary authentication 10.0.100.111 key simple password


[Comware7-radius-radius-auth]primary accounting ?
  STRING<1-253>  Host name
  X.X.X.X        IP address
  ipv6           Specify an IPv6 address

[Comware7-radius-radius-auth]primary accounting 10.0.100.111 ?
  INTEGER<1-65535>  Accounting port number, generally is 1813
  key               Specify the shared key for secure communication with the
                    server
  vpn-instance      Specify a VPN instance
  <cr>

[Comware7-radius-radius-auth]primary accounting 10.0.100.111 key ?
  cipher  Specify a ciphertext key
  simple  Specify a plaintext key

[Comware7-radius-radius-auth]primary accounting 10.0.100.111 key simple ?
  STRING<1-64>  Plaintext key string

[Comware7-radius-radius-auth]primary accounting 10.0.100.111 key simple password ?
  INTEGER<1-65535>  Accounting port number, generally is 1813
  vpn-instance      Specify a VPN instance
  <cr>

[Comware7-radius-radius-auth]primary accounting 10.0.100.111 key simple password


[Comware7-radius-radius-auth]user-name-format ?
  keep-original   User name unchanged
  with-domain     User name like XXX@XXX
  without-domain  User name like XXX
```

```
[Comware7-radius-radius-auth]user-name-format without-domain ?
  <cr>

[Comware7-radius-radius-auth]user-name-format without-domain


[Comware7]domain lab
New Domain added.

[Comware7-isp-lab]?
Isp view commands:
  accounting               Specify accounting scheme
  authentication           Specify authentication scheme
  authorization            Specify authorization scheme
  authorization-attribute  Configure authorization attributes of the domain
  cfd                      Connectivity Fault Detection (CFD) module
  diagnostic-logfile       Diagnostic log file configuration
  display                  Display current system information
  logfile                  Log file configuration
  monitor                  System monitor
  ping                     Ping function
  quit                     Exit from current command view
  return                   Exit to User View
  save                     Save current configuration
  security-logfile         Security log file configuration
  state                    Specify state of domain
  tracert                  Tracert function
  undo                     Cancel current setting

[Comware7-isp-lab]authentication ?
  advpn       Specify AAA configuration for ADVPN user
  default     Specify default AAA configuration for all types of users
  ike         Specify AAA configuration for IKE user
  lan-access  Specify AAA configuration for lan-access service
  login       Specify AAA configuration for login user
  portal      Specify AAA configuration for PORTAL user
  ppp         Specify AAA configuration for PPP user
  super       Specify AAA configuration for super user

[Comware7-isp-lab]authentication default ?
  hwtacacs-scheme  Specify HWTACACS scheme
  ldap-scheme      Specify LDAP scheme
  local            Specify local scheme
  none             Specify none scheme
  radius-scheme    Specify RADIUS scheme

[Comware7-isp-lab]authentication default radius-scheme ?
  STRING<1-32>  Scheme name

[Comware7-isp-lab]authentication default radius-scheme radius-auth ?
  hwtacacs-scheme  Specify HWTACACS scheme
  local            Specify local scheme
  none             Specify none scheme
  <cr>

[Comware7-isp-lab]authentication default radius-scheme radius-auth

[Comware7-isp-lab]authorization default radius-scheme radius-auth

[Comware7-isp-lab]accounting default radius-scheme radius-auth


[Comware7]domain default enable lab
```

```
[Comware7]user-interface aux 0

[Comware7-line-aux0]authentication-mode ?
  none      Login without authentication
  password  Password authentication
  scheme    Authentication use AAA

[Comware7-line-aux0]authentication-mode scheme ?
  <cr>

[Comware7-line-aux0]authentication-mode scheme


[Comware7]user-interface vty 0 63

[Comware7-line-vty0-63]authentication-mode ?
  none      Login without authentication
  password  Password authentication
  scheme    Authentication use AAA

[Comware7-line-vty0-63]authentication-mode scheme ?
  <cr>

[Comware7-line-vty0-63]authentication-mode scheme


[Comware7-line-vty0-63]user-role ?
  STRING<1-63>      User role name
  network-admin
  network-operator
  level-0
  level-1
  level-2
  level-3
  level-4
  level-5
  level-6
  level-7
  level-8
  level-9
  level-10
  level-11
  level-12
  level-13
  level-14
  level-15
  security-audit

[Comware7-line-vty0-63]user-role network-admin ?
  <cr>

[Comware7-line-vty0-63]user-role network-admin


[Comware7]display radius ?
  scheme      RADIUS scheme information
  statistics  Statistics information

[Comware7]display radius scheme ?
  >             Redirect it to a file
  >>            Redirect it to a file in append mode
```

```
  STRING<1-32>  Name of RADIUS scheme
  |             Matching output
  <cr>

[Comware7]display radius scheme radius-auth
RADIUS scheme name: radius-auth
  Index: 1
  Primary Auth Server:
    Host name: Not Configured
    IP  : 10.0.100.111                            Port: 1812   State: Active
    VPN : Not configured
  Primary Acct Server:
    Host name: Not Configured
    IP  : 10.0.100.111                            Port: 1813   State: Active
    VPN : Not configured

  Accounting-On function                     : Disabled
    Retransmission times                     : 50
    Retransmission interval(seconds)         : 3
  Timeout Interval(seconds)                  : 3
  Retransmission Times                       : 3
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)               : 5
  Realtime Accounting Interval(minutes)      : 12
  NAS IP Address                             : Not configured
  VPN                                        : Not configured
  User Name Format                           : Without-domain
  Data flow unit                             : Byte
  Packet unit                                : One
  Attribute 15 check-mode                    : Strict


[Comware7]display radius statistics ?
  >     Redirect it to a file
  >>    Redirect it to a file in append mode
  |     Matching output
  <cr>

[Comware7]display radius statistics

                                 Auth.         Acct.       SessCtrl.
          Request Packet:          7            14             0
            Retry Packet:          0             0             -
          Timeout Packet:          0             0             -
        Access Challenge:          0             -             -
           Account Start:          -             7             -
          Account Update:          -             0             -
            Account Stop:          -             7             -
       Terminate Request:          -             -             0
              Set Policy:          -             -             0
    Packet With Response:          7            14             0
 Packet Without Response:          0             0             -
          Access Rejects:          0             -             -
          Dropped Packet:          0             0             0
          Check Failures:          0             0             0
```

Cisco

```
Cisco(config)#aaa ?
  new-model  Enable NEW access control commands and functions.(Disables OLD
             commands.)

Cisco(config)#aaa new-model
```

```
Cisco(config)#radius-server ?
  accounting          Accounting information configuration
  attribute           Customize selected radius attributes
  authorization       Authorization processing information
  backoff             Retry backoff pattern(Default is retransmits with
                      constant delay)
  cache               AAA auth cache default server group
  challenge-noecho    Data echoing to screen is disabled during
                      Access-Challenge
  configure-nas       Attempt to upload static routes and IP pools at startup
  dead-criteria       Set the criteria used to decide when a radius server is
                      marked dead
  deadtime            Time to stop using a server that doesn't respond
  directed-request    Allow user to specify radius server to use with `@server'
  domain-stripping    Strip the domain from the username
  host                Specify a RADIUS server
  key                 encryption key shared with the radius servers
  load-balance        Radius load-balancing options.
  optional-passwords  The first RADIUS request can be made without requesting a
                      password
  retransmit          Specify the number of retries to active server
  retry               Specify how the next packet is sent after timeout.
  source-ports        source ports used for sending out RADIUS requests
  throttle            Throttle requests to radius server
  timeout             Time to wait for a RADIUS server to reply
  transaction         Specify per-transaction parameters
  unique-ident        Higher order bits of Acct-Session-Id
  vsa                 Vendor specific attribute configuration

Cisco(config)#radius-server host ?
  Hostname or A.B.C.D  IP address of RADIUS server

Cisco(config)#radius-server host 10.0.100.111 ?
  acct-port     UDP port for RADIUS accounting server (default is 1646)
  alias         1-8 aliases for this server (max. 8)
  auth-port     UDP port for RADIUS authentication server (default is 1645)
  backoff       Retry backoff pattern (Default is retransmits with constant
                delay)
  key           per-server encryption key (overrides default)
  key-wrap      per-server keywrap configuration
  non-standard  Parse attributes that violate the RADIUS standard
  pac           Generate per-server Protected Access Credential key
  retransmit    Specify the number of retries to active server (overrides
                default)
  test          Configure server automated testing.
  timeout       Time to wait for this RADIUS server to reply (overrides
                default)
  <cr>

Cisco(config)#radius-server host 10.0.100.111 auth-port ?
  <0-65535>  Port number

Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 ?
  acct-port     UDP port for RADIUS accounting server (default is 1646)
  auth-port     UDP port for RADIUS authentication server (default is 1645)
  backoff       Retry backoff pattern (Default is retransmits with constant
                delay)
  key           per-server encryption key (overrides default)
  key-wrap      per-server keywrap configuration
  non-standard  Parse attributes that violate the RADIUS standard
  pac           Generate per-server Protected Access Credential key
  retransmit    Specify the number of retries to active server (overrides
```

```
                 default)
  test           Configure server automated testing.
  timeout        Time to wait for this RADIUS server to reply (overrides
                 default)
  <cr>

Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port ?
  <0-65535>  Port number

Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 ?
  auth-port     UDP port for RADIUS authentication server (default is 1645)
  backoff       Retry backoff pattern (Default is retransmits with constant
                delay)
  key           per-server encryption key (overrides default)
  key-wrap      per-server keywrap configuration
  non-standard  Parse attributes that violate the RADIUS standard
  pac           Generate per-server Protected Access Credential key
  retransmit    Specify the number of retries to active server (overrides
                default)
  test          Configure server automated testing.
  timeout       Time to wait for this RADIUS server to reply (overrides
                default)
  <cr>

Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key ?
  0     Specifies an UNENCRYPTED key will follow
  7     Specifies HIDDEN key will follow
  LINE  The UNENCRYPTED (cleartext) server key

Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key password ?
  <cr>

Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key password


Cisco(config)#aaa ?
  accounting       Accounting configurations parameters.
  attribute        AAA attribute definitions
  authentication   Authentication configurations parameters.
  authorization    Authorization configurations parameters.
  cache            AAA cache definitions
  configuration    Authorization configuration parameters.
  dnis             Associate certain AAA parameters to a specific DNIS number
  group            AAA group definitions
  local            AAA Local Authen/Authz Method Lists
  local            AAA Local method options
  max-sessions     Adjust initial hash size for estimated max sessions
  memory           AAA memory parameters
  nas              NAS specific configuration
  new-model        Enable NEW access control commands and functions.(Disables
                   OLD commands.)
  pod              POD processing
  policy           AAA policy parameters
  server           Local AAA server
  service-profile  Service-Profile parameters
  session-id       AAA Session ID
  traceback        Traceback recording
  user             AAA user definitions

Cisco(config)#aaa authentication ?
  arap             Set authentication lists for arap.
  attempts         Set the maximum number of authentication attempts
  banner           Message to use when starting login/authentication.
```

```
  dot1x            Set authentication lists for IEEE 802.1x.
  enable           Set authentication list for enable.
  eou              Set authentication lists for EAPoUDP
  fail-message     Message to use for failed login/authentication.
  login            Set authentication lists for logins.
  password-prompt  Text to use when prompting for a password
  ppp              Set authentication lists for ppp.
  sgbp             Set authentication lists for sgbp.
  suppress         Do not send access request for a specific type of user.
  username-prompt  Text to use when prompting for a username

Cisco(config)#aaa authentication login ?
  WORD     Named authentication list (max 31 characters, longer will be
           rejected).
  default  The default authentication list.

Cisco(config)#aaa authentication login default ?
  cache          Use Cached-group
  enable         Use enable password for authentication.
  group          Use Server-group
  krb5           Use Kerberos 5 authentication.
  krb5-telnet    Allow logins only if already authenticated via Kerberos V
                 Telnet.
  line           Use line password for authentication.
  local          Use local username authentication.
  local-case     Use case-sensitive local username authentication.
  none           NO authentication.
  passwd-expiry  enable the login list to provide password aging support

Cisco(config)#aaa authentication login default group ?
  WORD     Server-group name
  ldap     Use list of all LDAP hosts.
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.

Cisco(config)#aaa authentication login default group radius ?
  cache       Use Cached-group
  enable      Use enable password for authentication.
  group       Use Server-group
  krb5        Use Kerberos 5 authentication.
  line        Use line password for authentication.
  local       Use local username authentication.
  local-case  Use case-sensitive local username authentication.
  none        NO authentication.
  <cr>

Cisco(config)#aaa authentication login default group radius local

Cisco(config)#aaa authentication enable default group radius local


Cisco(config)#line vty 0 15

Cisco(config-line)#login ?
  authentication  Authentication parameters.


Cisco(config-line)#login authentication ?
  WORD     Use an authentication list with this name.
  default  Use the default authentication list.


Cisco(config-line)#login authentication default ?
```

```
  <cr>

Cisco(config-line)#login authentication default


Cisco#show aaa servers

RADIUS: id 6, priority 1, host 10.0.100.111, auth-port 1812, acct-port 1813
     State: current UP, duration 171s, previous duration 0s
     Dead: total time 0s, count 0
     Quarantined: No
     Authen: request 3, timeouts 0, failover 0, retransmission 0
             Response: accept 1, reject 1, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 4956344ms
             Transaction: success 3, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Author: request 0, timeouts 0, failover 0, retransmission 0
             Response: accept 0, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Account: request 0, timeouts 0, failover 0, retransmission 0
             Request: start 0, interim 0, stop 0
             Response: start 0, interim 0, stop 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Elapsed time since counters last cleared: 2m
     Estimated Outstanding Access Transactions: 0
     Estimated Outstanding Accounting Transactions: 0
     Estimated Throttled Access Transactions: 0
     Estimated Throttled Accounting Transactions: 0
     Maximum Throttled Transactions: access 0, accounting 0
     Requests per minute past 24 hours:
             high - 0 hours, 1 minutes ago: 2
             low  - 0 hours, 3 minutes ago: 0
             average: 0


Cisco#show radius server-group radius
Server group radius
    Sharecount = 1  sg_unconfigured = FALSE
    Type = standard  Memlocks = 1
    Server(10.0.100.111:1812,1813) Transactions:
    Authen: 2   Author: 0       Acct: 0
    Server_auto_test_enabled: FALSE
     Keywrap enabled: FALSE

Cisco#show radius statistics
                                  Auth.      Acct.       Both
         Maximum inQ length:         NA         NA          1
       Maximum waitQ length:         NA         NA          1
       Maximum doneQ length:         NA         NA          1
       Total responses seen:         57          0         57
     Packets with responses:         17          0         17
  Packets without responses:         10          0         10
  Access Rejects           :         41
 Average response delay(ms):       2024          0       2024
 Maximum response delay(ms):       2148          0       2148
  Number of Radius timeouts:         40          0         40
       Duplicate ID detects:          0          0          0
 Buffer Allocation Failures:          0          0          0
Maximum Buffer Size (bytes):         89          0         89
```

```
Malformed Responses        :          0          0          0
Bad Authenticators         :          0          0          0
Unknown Responses          :          0          0          0
 Source Port Range: (2 ports only)
 1645 - 1646
 Last used Source Port/Identifier:
 1645/27
 1646/0

  Elapsed time since counters last cleared: 4h9m
```

b) Privilege Mode

This feature provides a dedicated login at a specific user level, based on the reply the authentication server sends to the switch.

Must execute the basic configuration (section a) first.

ArubaOS-Switch	Comware	Cisco
(Requires special configuration on the RADIUS server)	(Requires special configuration on the RADIUS server) No additional Comware RADIUS configuration required to support this option.	(Requires special configuration on the RADIUS server)
`ArubaOS-Switch(config)# aaa authentication login privilege-mode`		
		`Cisco(config)#aaa authorization console`
		`Cisco(config)#aaa authorization exec default group radius`
`ArubaOS-Switch# show authentication`		

ArubaOS-Switch

(Requires special configuration on the RADIUS server)

```
ArubaOS-Switch(config)# aaa ?
accounting             Configure accounting parameters on the switch.
 authentication         Configure authentication parameters on the switch.
 authorization          Configure authorization parameters on the switch.
 port-access            Configure 802.1X (Port Based Network Access), MAC address based
                        network access, or web authentication based network access on the
                        device.
 server-group           Place the RADIUS server into the RADIUS server group.

ArubaOS-Switch(config)# aaa authentication ?
allow-vlan             Configure authenticator ports to apply VLAN changes immediately.
 console                Configure authentication mechanism used to control access to the
                        switch console.
 disable-username       Bypass the username during authentication while accessing the
                        switch to get Manager or Operator access.
 local-user             Create or remove a local user account.
 lockout-delay          The number of seconds after repeated login failures before a user
                        may again attempt login.
 login                  Specify that switch respects the authentication server's privilege
                        level.
 mac-based              Configure authentication mechanism used to control mac-based port
                        access to the switch.
 num-attempts           The number of login attempts allowed.
 port-access            Configure authentication mechanism used to control access to the
                        network.
 ssh                    Configure authentication mechanism used to control SSH access to
                        the switch.
 telnet                 Configure authentication mechanism used to control telnet access
```

```
                        to the switch.
 web                    Configure authentication mechanism used to control web access to
                        the switch.
 web-based              Configure authentication mechanism used to control web-based port
                        access to the switch.

ArubaOS-Switch(config)# aaa authentication login ?
 privilege-mode         Specify that switch respects the authentication server's privilege
                        level.

ArubaOS-Switch(config)# aaa authentication login privilege-mode ?
 <cr>

ArubaOS-Switch(config)# aaa authentication login privilege-mode


ArubaOS-Switch# show authentication

Status and Counters - Authentication Information

  Login Attempts : 3
  Lockout Delay : 0
  Respect Privilege : Enabled
  Bypass Username For Operator and Manager Access : Disabled

                  | Login      Login        Login
  Access Task     | Primary    Server Group Secondary
  -------------- + ---------- ------------ ----------
  Console         | Radius     radius       Local
  Telnet          | Radius     radius       None
  Port-Access     | Local                   None
  Webui           | Radius     radius       None
  SSH             | Radius     radius       None
  Web-Auth        | ChapRadius radius       None
  MAC-Auth        | ChapRadius radius       None
  SNMP            | Local                   None
  Local-MAC-Auth  | Local      radius       None
                  | Local                   None

                  | Enable     Enable       Enable
  Access Task     | Primary    Server Group Secondary
  -------------- + ---------- ------------ ----------
  Console         | Radius     radius       Local
  Telnet          | Radius     radius       None
  Webui           | Radius     radius       None
  SSH             | Radius     radius       None
```

Comware

(Requires special configuration on the RADIUS server)

No additional Comware RADIUS configuration required to support this option.

Cisco

(Requires special configuration on the RADIUS server)

```
Cisco(config)#aaa ?
  accounting       Accounting configurations parameters.
  attribute        AAA attribute definitions
  authentication   Authentication configurations parameters.
  authorization    Authorization configurations parameters.
  cache            AAA cache definitions
  configuration    Authorization configuration parameters.
```

```
  dnis             Associate certain AAA parameters to a specific DNIS number
  group            AAA group definitions
  local            AAA Local Authen/Authz Method Lists
  local            AAA Local method options
  max-sessions     Adjust initial hash size for estimated max sessions
  memory           AAA memory parameters
  nas              NAS specific configuration
  new-model        Enable NEW access control commands and functions.(Disables
                   OLD commands.)
  pod              POD processing
  policy           AAA policy parameters
  server           Local AAA server
  service-profile  Service-Profile parameters
  session-id       AAA Session ID
  traceback        Traceback recording
  user             AAA user definitions

Cisco(config)#aaa authorization ?
  auth-proxy           For Authentication Proxy Services
  cache                For AAA cache configuration
  commands             For exec (shell) commands.
  config-commands      For configuration mode commands.
  configuration        For downloading configurations from AAA server
  console              For enabling console authorization
  credential-download  For downloading EAP credential from Local/RADIUS/LDAP
  exec                 For starting an exec (shell).
  multicast            For downloading Multicast configurations from an AAA
                       server
  network              For network services. (PPP, SLIP, ARAP)
  policy-if            For diameter policy interface application.
  prepaid              For diameter prepaid services.
  radius-proxy         For proxying radius packets
  reverse-access       For reverse access connections
  subscriber-service   For iEdge subscriber services (VPDN etc)
  template             Enable template authorization

Cisco(config)#aaa authorization console ?
  <cr>

Cisco(config)#aaa authorization exec ?
  WORD     Named authorization list (max 31 characters, longer will be
           rejected).
  default  The default authorization list.

Cisco(config)#aaa authorization exec default ?
  cache             Use Cached-group
  group             Use server-group.
  if-authenticated  Succeed if user has authenticated.
  krb5-instance     Use Kerberos instance privilege maps.
  local             Use local database.
  none              No authorization (always succeeds).

Cisco(config)#aaa authorization exec default group ?
  WORD     Server-group name
  ldap     Use list of all LDAP hosts.
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.

Cisco(config)#aaa authorization exec default group radius ?
  cache             Use Cached-group
  group             Use server-group.
  if-authenticated  Succeed if user has authenticated.
  krb5-instance     Use Kerberos instance privilege maps.
```

```
  local             Use local database.
  none              No authorization (always succeeds).
  <cr>


Cisco(config)#aaa authorization exec default group radius
```

c) Commands Authorization

This feature provides a specific set of commands that a user can (or cannot) execute upon login at a specific user level, based on the reply the authentication server sends to the switch.

Must execute the basic configuration (section a) first.

ArubaOS-Switch	Comware5	Cisco
(Requires special configuration on the RADIUS server)	(Requires special configuration on the RADIUS server)	Not an available feature

`ArubaOS-Switch(config)# aaa authorization commands radius`	`[Comware5]user-interface vty 0 15`
	
	`[Comware5-ui-vty0-15]command authorization`	

	Comware7	
	(Requires special configuration on the RADIUS server)	

	`[Comware7]user-interface vty 0 63`
	
	`[Comware5-ui-vty0-63]command authorization`	

`ArubaOS-Switch# show authorization`		

ArubaOS-Switch

(Requires special configuration on the RADIUS server)

```
ArubaOS-Switch(config)# aaa authorization commands radius

ArubaOS-Switch# show authorization

 Status and Counters - Authorization Information

  Type     | Method
  -------- + ------
  Commands | Radius
```

Comware5

(Requires special configuration on the RADIUS server)

```
[Comware5-ui-vty0-15]command ?
  accounting     Record valid commands on server
  authorization  Authorization needed before running a command

[Comware5-ui-vty0-15]command authorization ?
  <cr>

[Comware5-ui-vty0-15]command authorization
```

Comware7

(Requires special configuration on the RADIUS server)

```
[Comware7-line-vty0-63]command ?
  accounting     Enable command accounting
  authorization  Enable command authorization

[Comware7-line-vty0-63]command authorization ?
  <cr>

[Comware7-line-vty0-63]command authorization
```

Cisco

Not an available feature

d) RADIUS Accounting

RADIUS accounting was started in the basic configuration section a. These additional options provide specific reporting information to the RADIUS server.

Must execute the basic configuration (section a) first.

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# aaa accounting exec start-stop radius	(Basic support only; no other specific feature support)	Cisco(config)#aaa accounting exec default start-stop group radius
ArubaOS-Switch(config)# aaa accounting network start-stop radius		Cisco(config)#aaa accounting network default start-stop group radius
ArubaOS-Switch(config)# aaa accounting system start-stop radius		Cisco(config)#aaa accounting system default start-stop group radius
ArubaOS-Switch(config)# aaa accounting commands stop-only radius		
ArubaOS-Switch# show radius accounting		
ArubaOS-Switch# show accounting		Cisco#show aaa user all
ArubaOS-Switch# show accounting sessions		

ArubaOS-Switch

```
ArubaOS-Switch(config)# aaa accounting ?
 commands              Configure 'commands' type of accounting.
 exec                  Configure 'exec' type of accounting.
 network               Configure 'network' type of accounting.
 session-id            Configure accounting sessions identification scheme.
 suppress              Do not generate accounting records for a specific type of user.
 system                Configure 'system' type of accounting.
 update                Configure update accounting records mechanism.

ArubaOS-Switch(config)# aaa accounting exec ?
 start-stop            Send start and stop record accounting notice.
 stop-only             Send stop record accounting notice only.

ArubaOS-Switch(config)# aaa accounting exec start-stop ?
 radius                Use RADIUS protocol as accounting method.
 syslog                Use syslog protocol as accounting method.

ArubaOS-Switch(config)# aaa accounting exec start-stop radius ?
 server-group          Specify the server group to use.
 <cr>

ArubaOS-Switch(config)# aaa accounting exec start-stop radius


ArubaOS-Switch(config)# aaa accounting network start-stop radius


ArubaOS-Switch(config)# aaa accounting system start-stop radius
```

```
ArubaOS-Switch(config)# aaa accounting commands stop-only radius

ArubaOS-Switch# show radius accounting

 Status and Counters - RADIUS Accounting Information

  NAS Identifier           : ArubaOS-Switch
  Invalid Server Addresses : 0
                  UDP
  Server IP Addr  Port Timeouts   Requests   Responses
  --------------- ---- ---------- ---------- ----------
  10.0.100.111    1813 5          6          5


ArubaOS-Switch# show accounting ?
 sessions              Show accounting data for all active sessions.
 <cr>

ArubaOS-Switch# show accounting

 Status and Counters - Accounting Information

  Interval(min) : 0
  Suppress Empty User : No
  Sessions Identification : Unique

  Type     | Method Mode       Server Group
  -------- + ------ ---------- ------------
  Network  | Radius Start-Stop radius
  Exec     | Radius Start-Stop radius
  System   | Radius Start-Stop radius
  Commands | Radius Stop-Only  radius


ArubaOS-Switch# show accounting sessions ?
 <cr>

ArubaOS-Switch# show accounting sessions

Active Accounted actions on SWITCH, User (n/a) Priv (n/a),
 Acct-Session-Id 0x002700000001, System Accounting record, 00:01:14 Elapsed
 system event 'Accounting On'
```

Comware

(Basic support only, no other specific feature support)

Cisco

```
Cisco(config)#aaa accounting ?
  auth-proxy        For authentication proxy events.
  commands          For exec (shell) commands.
  connection        For outbound connections. (telnet, rlogin)
  delay-start       Delay PPP Network start record until peer IP address is
                    known.
  dot1x             For dot1x sessions.
  exec              For starting an exec (shell).
  gigawords         64 bit interface counters to support Radius attributes 52 &
                    53.
  include           Include attributes in accounting records unconditionally
  jitter            Set jitter parameters for periodic interval
  multicast         For multicast accounting.
  nested            When starting PPP from EXEC, generate NETWORK records
```

```
                      before EXEC-STOP record.
  network             For network services. (PPP, SLIP, ARAP)
  redundancy          AAA platform redundancy accounting behavior
  send                Send records to accounting server.
  session-duration    Set the preference for calculating session durations
  suppress            Do not generate accounting records for a specific type of
                      user.
  system              For system events.
  update              Enable accounting update records.
  vrrs                For VRRS accounting.

Cisco(config)#aaa accounting exec ?
  WORD     Named Accounting list (max 31 characters, longer will be rejected).
  default  The default accounting list.

Cisco(config)#aaa accounting exec default ?
  none        No accounting.
  start-stop  Record start and stop without waiting
  stop-only   Record stop when service terminates.
  <cr>

Cisco(config)#aaa accounting exec default start-stop ?
  broadcast  Use Broadcast for Accounting
  group      Use Server-group

Cisco(config)#aaa accounting exec default start-stop group ?
  WORD     Server-group name
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.

Cisco(config)#aaa accounting exec default start-stop group radius ?
  group  Use Server-group
  <cr>

Cisco(config)#aaa accounting exec default start-stop group radius


Cisco(config)#aaa accounting network default start-stop group radius


Cisco(config)#aaa accounting system default start-stop group radius

Cisco#show aaa user all
--------------------------------------------------
Unique id 1 is currently in use.
Accounting:
  log=0x18001
  Events recorded :
    CALL START
    INTERIM START
    INTERIM STOP
  update method(s) :
    NONE
  update interval = 0
  Outstanding Stop Records : 0
  Dynamic attribute list:
    03802C08 0 00000001 connect-progress(44) 4 No Progress
    03802C1C 0 00000001 pre-session-time(272) 4 269025(41AE1)
    03802C30 0 00000001 elapsed_time(339) 4 0(0)
    03802C44 0 00000001 pre-bytes-in(268) 4 0(0)
```

```
    03802C58 0 00000001 pre-bytes-out(269) 4 0(0)
    039A269C 0 00000001 pre-paks-in(270) 4 0(0)
    039A26B0 0 00000001 pre-paks-out(271) 4 0(0)
  No data for type EXEC
  No data for type CONN
  NET: Username=(n/a)
...
```

Chapter 11 TACACS+/HWTACACS Authentication for Switch Management

This chapter covers the commands you use to authenticate management users to a Terminal Access Controller Access Control System (TACACS) server.

TACACS is described in RFC 927 and RFC 1492, and TACACS+ is described in draft-grant-tacacs-02 whereby Cisco extended the TACACS definition by adding security features and the capability to split the AAA server into three separate servers and/or functions.

Huawei Terminal Access Controller Access Control System (HWTACACS) is an enhanced security protocol based on TACACS (RFC 1492). Similar to Remote Authentication Dial-In User Service (RADIUS), it uses a client/server model for information exchange between the Network Access Server (NAS) and the HWTACACS server.

HWTACACS uses TCP port 49 for authentication, authorization, and accounting.

RADIUS also provides authentication, authorization, and accounting services. HWTACACS and RADIUS have many features in common, including a client/server model, the use of shared keys for user information security, and flexibility and extensibility. Their differences are listed in the following table:

HWTACACS	RADIUS
HWTACACS uses TCP, providing more reliable network transmission.	RADIUS uses UDP, providing higher transport efficiency.
It encrypts the entire packet, except for the HWTACACS header.	It encrypts only the user password field in an authentication packet.
Protocol packets are complicated and authorization is independent of authentication. You can deploy authentication and authorization on different HWTACACS servers.	Protocol packets are simple and the authorization process is combined with the authentication process.
HWTACACS upports authorization of configuration commands. A user can use commands that are at or below the user's level or are authorized by the HWTACACS server.	RADIUS does not support authorization of configuration commands. A user can use all the commands at our below the user's level. (ArubaOS-Switch has this as a feature using VSA configuration parameters on the RADIUS server that are passed to the NAS.)

a) Basic Configuration

ArubaOS-Switch	Comware5	Cisco
	(If you are planning to use Telnet or SSH, you should configure those features before you configure AAA support.) (See notes below concerning login procedures for HWTACACS.)	
	`[Comware5]hwtacacs scheme tacacs-auth`	`Cisco(config)#aaa new-model`

ArubaOS-Switch(config)# tacacs-server host 10.0.100.111 key password	[Comware5-hwtacacs-tacacs-auth]primary authentication 10.0.100.111 key simple password [Comware5-hwtacacs-tacacs-auth]primary authorization 10.0.100.111 key simple password [Comware5-hwtacacs-tacacs-auth]primary accounting 10.0.100.111 key simple password [Comware5-hwtacacs-tacacs-auth]user-name-format without-domain	Cisco(config)#tacacs-server host 10.0.100.111 key password
ArubaOS-Switch(config)# aaa authentication console login tacacs local		Cisco(config)#aaa authentication login default group tacacs+ local
ArubaOS-Switch(config)# aaa authentication console enable tacacs local		Cisco(config)#aaa authentication enable default group tacacs+ local
ArubaOS-Switch(config)# aaa authentication telnet login tacacs none		Cisco(config)#aaa authentication login default group tacacs+
ArubaOS-Switch(config)# aaa authentication telnet enable tacacs none		Cisco(config)#aaa authentication enable default group tacacs+
ArubaOS-Switch(config)# aaa authentication ssh login tacacs none		Cisco(config)#aaa authentication login default group tacacs+
ArubaOS-Switch(config)# aaa authentication ssh enable tacacs none		Cisco(config)#aaa authentication enable default group tacacs+
	[Comware5]domain tacacs [Comware5-isp-tacacs]authentication default hwtacacs-scheme tacacs-auth [Comware5-isp-tacacs]authorization default hwtacacs-scheme tacacs-auth [Comware5-isp-tacacs]accounting default hwtacacs-scheme tacacs-auth	
	[Comware5]domain default enable tacacs	
	[Comware5]user-interface aux 0	
	[Comware5-ui-aux0]authentication-mode scheme	
	[Comware5]user-interface vty 0 15	Cisco(config)#line vty 0 15

	[Comware5-ui-vty0-15]authentication-mode scheme	Cisco(config-line)#login authentication default
ArubaOS-Switch# show tacacs	[Comware5]display hwtacacs [Comware5]display hwtacacs tacacs-auth statistics	Cisco#show tacacs
ArubaOS-Switch# show authentication		
	Comware7	
	(If you are planning to use Telnet or SSH, you should configure those features before you configure AAA support.) (See notes below concerning login procedures for HWTACACS.)	
	[Comware7]hwtacacs scheme tacacs-auth	
	[Comware7-hwtacacs-tacacs-auth]primary authentication 10.0.100.111 key simple password [Comware7-hwtacacs-tacacs-auth]primary authorization 10.0.100.111 key simple password [Comware7-hwtacacs-tacacs-auth]primary accounting 10.0.100.111 key simple password [Comware7-hwtacacs-tacacs-auth]user-name-format without-domain	
	[Comware7]domain tacacs [Comware7-isp-tacacs]authentication default hwtacacs-scheme tacacs-auth [Comware7-isp-tacacs]authorization default hwtacacs-scheme tacacs-auth [Comware7-isp-tacacs]accounting default hwtacacs-scheme tacacs-auth	
	[Comware7]domain default enable tacacs	
	[Comware7]user-interface aux 0	

	[Comware7-line-aux0]authentication-mode scheme	
	[Comware7]user-interface vty 0 63	
	[Comware7-line-vty0-63]authentication-mode scheme	
	[Comware7]display hwtacacs [Comware7]display hwtacacs scheme tacacs-auth statistics	

ArubaOS-Switch

```
ArubaOS-Switch(config)# tacacs-server ?
host                   IP address of the server to use.
 key                    Global encryption key. If in enhanced secure-mode, you will be
                        prompted for the key.
 timeout                Server timeout interval.

ArubaOS-Switch(config)# tacacs-server host ?
 IP-ADDR                Enter an IP address.

ArubaOS-Switch(config)# tacacs-server host 10.0.100.111 ?
 key                    Encryption key to use with server. If in enhanced secure-mode, you
                        will be prompted for the key.
 oobm                   Use OOBM interface to connect to server
 <cr>

ArubaOS-Switch(config)# tacacs-server host 10.0.100.111 key ?
 KEY
 oobm                   Use OOBM interface to connect to server

ArubaOS-Switch(config)# tacacs-server host 10.0.100.111 key password ?
 oobm                   Use OOBM interface to connect to server
 <cr>

ArubaOS-Switch(config)# tacacs-server host 10.0.100.111 key password


ArubaOS-Switch(config)# aaa ?
 accounting             Configure accounting parameters on the switch.
 authentication         Configure authentication parameters on the switch.
 authorization          Configure authorization parameters on the switch.
 port-access            Configure 802.1X (Port Based Network Access), MAC address based
                        network access, or web authentication based network access on the
                        device.
 server-group           Place the RADIUS server into the RADIUS server group.

ArubaOS-Switch(config)# aaa authentication ?
 allow-vlan             Configure authenticator ports to apply VLAN changes immediately.
 console                Configure authentication mechanism used to control access to the
                        switch console.
 disable-username       Bypass the username during authentication while accessing the
                        switch to get Manager or Operator access.
 local-user             Create or remove a local user account.
 lockout-delay          The number of seconds after repeated login failures before a user
                        may again attempt login.
 login                  Specify that switch respects the authentication server's privilege
```

```
                        level.
 mac-based              Configure authentication mechanism used to control mac-based port
                        access to the switch.
 num-attempts           The number of login attempts allowed.
 port-access            Configure authentication mechanism used to control access to the
                        network.
 ssh                    Configure authentication mechanism used to control SSH access to
                        the switch.
 telnet                 Configure authentication mechanism used to control telnet access
                        to the switch.
 web                    Configure authentication mechanism used to control web access to
                        the switch.
 web-based              Configure authentication mechanism used to control web-based port
                        access to the switch.

ArubaOS-Switch(config)# aaa authentication console ?
 enable                 Configure access to the privileged mode commands.
 login                  Configure login access to the switch.

ArubaOS-Switch(config)# aaa authentication console login ?
 local                  Use local switch user/password database.
 tacacs                 Use TACACS+ server.
 radius                 Use RADIUS server.
 peap-mschapv2          Use RADIUS server with PEAP-MSChapv2.

ArubaOS-Switch(config)# aaa authentication console login tacacs ?
 local                  Use local switch user/password database.
 none                   Do not use backup authentication methods.
 authorized             Allow access without authentication.
 server-group           Specify the server group to use.
 <cr>

ArubaOS-Switch(config)# aaa authentication console login tacacs local ?
 <cr>

ArubaOS-Switch(config)# aaa authentication console login tacacs local

ArubaOS-Switch(config)# aaa authentication console enable tacacs local

ArubaOS-Switch(config)# aaa authentication telnet login tacacs none

ArubaOS-Switch(config)# aaa authentication telnet enable tacacs none

ArubaOS-Switch(config)# aaa authentication ssh login tacacs none

ArubaOS-Switch(config)# aaa authentication ssh enable tacacs none



ArubaOS-Switch# show tacacs

 Status and Counters - TACACS Information

  Timeout : 5
  Source IP Selection : 10.0.111.21
  Encryption Key :


  Server IP Addr  Opens  Closes Aborts Errors Pkts Rx Pkts Tx OOBM
  --------------- ------ ------ ------ ------ ------- ------- ----
  10.0.100.111    6      4      2      0      12      14      0
```

```
ArubaOS-Switch# show authentication

 Status and Counters - Authentication Information

  Login Attempts : 3
  Lockout Delay : 0
  Respect Privilege : Disabled
  Bypass Username For Operator and Manager Access : Disabled

                  | Login      Login        Login
  Access Task     | Primary    Server Group Secondary
  -------------- + ---------- ------------ ----------
  Console         | Tacacs                  Local
  Telnet          | Tacacs                  None
  Port-Access     | Local                   None
  Webui           | Local                   None
  SSH             | Tacacs                  None
  Web-Auth        | ChapRadius radius       None
  MAC-Auth        | ChapRadius radius       None
  SNMP            | Local                   None
  Local-MAC-Auth  | Local                   None
                  | Local                   None

                  | Enable     Enable       Enable
  Access Task     | Primary    Server Group Secondary
  -------------- + ---------- ------------ ----------
  Console         | Tacacs                  Local
  Telnet          | Tacacs                  None
  Webui           | Local                   None
  SSH             | Tacacs                  None
```

Comware5

(If you are planning to use Telnet or SSH, you should configure those features before you configure AAA support.)

Special note on using AAA authentication. By default Comware5 is expecting a user to login as "user@domain", this allows for multiple domain support.

In order to support a user to supply only their UID without the "@domain", the '`user-name-format without-domain`' parameter can be configured within the hwtacacs scheme, which allows Comware5 to send just a UID to the HWTACACS server.

```
[Comware5]hwtacacs ?
  nas-ip  Specify HWTACACS client IP address
  scheme  Specify HWTACACS server scheme

[Comware5]hwtacacs scheme ?
  STRING<1-32>  Scheme name

[Comware5]hwtacacs scheme tacacs-auth ?
  <cr>

[Comware5]hwtacacs scheme tacacs-auth
Create a new HWTACACS-server scheme

[Comware5-hwtacacs-tacacs_auth]?
Hwtacacs view commands:
  cfd                     Connectivity fault detection (IEEE 802.1ag)
  data-flow-format        Specify octet format
  display                 Display current system information
  key                     Key for HWTACACS-server template
```

```
  mtracert                Trace route to multicast source
  nas-ip                  Specify HWTACACS client IP address
  ping                    Ping function
  primary                 Specify primary server
  quit                    Exit from current command view
  retry                   Specify retransmit times of the stop-accounting
                          packet
  return                  Exit to User View
  save                    Save current configuration
  secondary               Specify server for secondary
  stop-accounting-buffer  Enable HWTACACS server accounting stop buffer
  timer                   Specify timer for HWTACACS
  tracert                 Trace route function
  undo                    Cancel current setting
  user-name-format        Specify user-name format sent to HWTACACS server
  vpn-instance            Specify VPN instance

[Comware5-hwtacacs-tacacs_auth]primary ?
  accounting      Specify HWTACACS accounting server
  authentication  Specify HWTACACS authentication server
  authorization   Specify HWTACACS authorization server

[Comware5-hwtacacs-tacacs_auth]primary authentication ?
  X.X.X.X  IP address

[Comware5-hwtacacs-tacacs_auth]primary authentication 10.0.100.111 ?
  INTEGER<1-65535>  Specify port for server
  key               Specify the shared key for secure communication with the
                    server
  vpn-instance      Specify VPN instance
  <cr>

[Comware5-hwtacacs-tacacs-auth]primary authentication 10.0.100.111 key ?
  STRING<1-255>  Plaintext key string
  cipher         Specify a ciphertext key
  simple         Specify a plaintext key

[Comware5-hwtacacs-tacacs-auth]primary authentication 10.0.100.111 key simple ?
  STRING<1-255>  Plaintext key string

[Comware5-hwtacacs-tacacs-auth]primary authentication 10.0.100.111 key simple password ?
  INTEGER<1-65535>  Specify port for server
  vpn-instance      Specify VPN instance
  <cr>

[Comware5-hwtacacs-tacacs-auth]primary authentication 10.0.100.111 key simple password

[Comware5-hwtacacs-tacacs-auth]primary authorization 10.0.100.111 key simple password

[Comware5-hwtacacs-tacacs-auth]primary accounting 10.0.100.111 key simple password


[Comware5-hwtacacs-tacacs-auth]user-name-format ?
  keep-original   User name unchanged
  with-domain     User name like XXX@XXX
  without-domain  User name like XXX

[Comware5-hwtacacs-tacacs-auth]user-name-format with-domain ?
  <cr>

[Comware5-hwtacacs-tacacs-auth]user-name-format without-domain
```

```
[Comware5]domain tacacs

[Comware5-isp-tacacs]?
Isp view commands:

  access-limit             Specify access limit of domain
  accounting               Specify accounting scheme
  authentication           Specify authentication scheme
  authorization            Specify authorization scheme
  authorization-attribute  Specify authorization attributes of domain
  cfd                      Connectivity fault detection (IEEE 802.1ag)
  display                  Display current system information
  dscp                     Specify a DSCP value for user packets of this domain
  idle-cut                 Specify idle-cut attribute of domain
  mtracert                 Trace route to multicast source
  ping                     Ping function
  quit                     Exit from current command view
  return                   Exit to User View
  save                     Save current configuration
  self-service-url         Specify self-service URL(Uniform Resource Locator)
                           of domain
  state                    Specify state of domain
  tracert                  Trace route function
  undo                     Cancel current setting

[Comware5-isp-tacacs]authentication ?
  default     Specify default AAA configuration
  lan-access  Specify lan-access AAA configuration
  login       Specify login AAA configuration
  portal      Specify portal AAA configuration
  super       Specify super AAA configuration

[Comware5-isp-tacacs]authentication default ?
  hwtacacs-scheme  Specify HWTACACS scheme
  local            Specify local scheme
  none             Specify none scheme
  radius-scheme    Specify RADIUS scheme

[Comware5-isp-tacacs]authentication default hwtacacs-scheme ?
  STRING<1-32>  Scheme name

[Comware5-isp-tacacs]authentication default hwtacacs-scheme tacacs-auth

[Comware5-isp-tacacs]authorization default hwtacacs-scheme tacacs-auth

[Comware5-isp-tacacs]accounting default hwtacacs-scheme tacacs-auth


[Comware5]domain default enable tacacs


[Comware5]user-interface aux 0

[Comware5-ui-aux0]authentication-mode ?
  none      Login without checking
  password  Authentication use password of user terminal interface
  scheme    Authentication use AAA

[Comware5-ui-aux0]authentication-mode scheme ?
  <cr>

[Comware5-ui-aux0]authentication-mode scheme
```

```
[Comware5]user-interface vty 0 15

[Comware5-ui-vty0-15]authentication-mode ?
  none      Login without checking
  password  Authentication use password of user terminal interface
  scheme    Authentication use AAA

[Comware5-ui-vty0-15]authentication-mode scheme ?
  <cr>

[Comware5-ui-vty0-15]authentication-mode scheme


[Comware5]display hwtacacs ?
  STRING<1-32>  Scheme name
  slot          Specify slot number
  |             Matching output
  <cr>

[Comware5]display hwtacacs
HWTACACS scheme name : tacacs-auth
  Primary Authen Server:
    IP: 10.0.100.111                            Port: 49     State: Active
    VPN instance   : Not configured
    Encryption Key : ******
  Primary Author Server:
    IP: 10.0.100.111                            Port: 49     State: Active
    VPN instance   : Not configured
    Encryption Key : ******
  Primary Account Server:
    IP: 10.0.100.111                            Port: 49     State: Active
    VPN instance   : Not configured
    Encryption Key : ******
  NAS IP address                                : Not configured
  Authentication key                            : Not configured
  Authorization key                             : Not configured
  Accounting key                                : Not configured
  VPN instance                                  : Not configured
  Quiet interval(min)                           : 5
  Realtime accounting interval(min)             : 12
  Response timeout interval(sec)                : 5
  Retransmission times of stop-accounting packet : 100
  Username format                               : without-domain
  Data flow unit                                : Byte
  Packet unit                                   : one
-------------------------------------------------------------------------
  Total 1 HWTACACS scheme(s).

[Comware5]display hwtacacs tacacs-auth statistics
Slot: 1
HWTACACS scheme name: tacacs-auth
Primary authentication server: 10.0.100.111
  HWTACACS server open number: 4
  HWTACACS server close number: 4
  HWTACACS authen client access request packet number: 4
  HWTACACS authen client access response packet number: 4
  HWTACACS authen client unknown type number: 0
  HWTACACS authen client timeout number: 0
  HWTACACS authen client packet dropped number: 0
  HWTACACS authen client access request change password number: 0
  HWTACACS authen client access request login number: 2
  HWTACACS authen client access request send authentication number: 0
```

```
  HWTACACS authen client access request send password number: 0
  HWTACACS authen client access connect abort number: 0
  HWTACACS authen client access connect packet number: 2
  HWTACACS authen client access response error number: 0
  HWTACACS authen client access response failure number: 0
  HWTACACS authen client access response follow number: 0
  HWTACACS authen client access response getdata number: 0
  HWTACACS authen client access response getpassword number: 2
  HWTACACS authen client access response getuser number: 0
  HWTACACS authen client access response pass number: 2
  HWTACACS authen client access response restart number: 0
  HWTACACS authen client malformed access response number: 0
  HWTACACS authen client round trip time(s): 1
Primary authorization server: 10.0.100.111
  HWTACACS server open number: 2
  HWTACACS server close number: 2
  HWTACACS author client request packet number: 2
  HWTACACS author client response packet number: 2
  HWTACACS author client timeout number: 0
  HWTACACS author client packet dropped number: 0
  HWTACACS author client unknown type number: 0
  HWTACACS author client request EXEC number: 2
  HWTACACS author client request PPP number: 0
  HWTACACS author client request VPDN number: 0
  HWTACACS author client response error number: 0
  HWTACACS author client response EXEC number: 2
  HWTACACS author client response PPP number: 0
  HWTACACS author client response VPDN number: 0
  HWTACACS author client round trip time(s): 0
Primary accounting server: 10.0.100.111
  HWTACACS server open number: 3
  HWTACACS server close number: 3
  HWTACACS account client request packet number: 3
  HWTACACS account client response packet number: 3
  HWTACACS account client unknown type number: 0
  HWTACACS account client timeout number: 0
  HWTACACS account client packet dropped number: 0
  HWTACACS account client request command level number: 0
  HWTACACS account client request connection number: 0
  HWTACACS account client request EXEC number: 3
  HWTACACS account client request network number: 0
  HWTACACS account client request system event number: 0
  HWTACACS account client request update number: 0
  HWTACACS account client response error number: 0
  HWTACACS account client round trip time(s): 0
```

Comware7

(If you are planning to use Telnet or SSH, you should configure those features before you configure AAA support.)

Special note on using AAA authentication. By default Comware is expecting a user to login as "user@domain", this allows for multiple domain support.

In order to support a user to supply only their UID without the "@domain", the '`user-name-format without-domain`' parameter can be configured within the hwtacacs scheme, which allows Comware to send just a UID to the HWTACACS server.

```
[Comware7]hwtacacs ?
  nas-ip  Specify the HWTACACS client IP address
  scheme  Specify HWTACACS scheme
```

```
[Comware7]hwtacacs scheme ?
  STRING<1-32>  HWTACACS scheme name

[Comware7]hwtacacs scheme tacacs-auth ?
  <cr>

[Comware7]hwtacacs scheme tacacs-auth
Create a new HWTACACS scheme.

[Comware7-hwtacacs-tacacs-auth]?
Hwtacacs protocol view commands:
  cfd                 Connectivity Fault Detection (CFD) module
  data-flow-format    Specify the data unit
  diagnostic-logfile  Diagnostic log file configuration
  display             Display current system information
  key                 Specify a key for secure HWTACACS communication
  logfile             Log file configuration
  monitor             System monitor
  nas-ip              Specify the HWTACACS client IP address
  ping                Ping function
  primary             Specify a primary HWTACACS server
  quit                Exit from current command view
  return              Exit to User View
  save                Save current configuration
  secondary           Specify a secondary HWTACACS server
  security-logfile    Security log file configuration
  timer               Specify timer parameters
  tracert             Tracert function
  undo                Cancel current setting
  user-name-format    Specify user-name format sent to HWTACACS server
  vpn-instance        Specify a VPN instance

[Comware7-hwtacacs-tacacs-auth]primary ?
  accounting      Specify the primary HWTACACS accounting server
  authentication  Specify the primary HWTACACS authentication server
  authorization   Specify the primary HWTACACS authorization server

[Comware7-hwtacacs-tacacs-auth]primary authentication ?
  STRING<1-253>  Host name
  X.X.X.X        IP address
  ipv6           Specify an IPv6 address

[Comware7-hwtacacs-tacacs-auth]primary authentication 10.0.100.111 ?
  INTEGER<1-65535>   port number, 49 by default
  key                Specify the shared key for secure communication with the
                     server
  single-connection  Transmit HWTACACS packets on an open TCP connection
  vpn-instance       Specify a VPN instance
  <cr>

[Comware7-hwtacacs-tacacs-auth]primary authentication 10.0.100.111 key ?
  cipher  Specify a ciphertext key
  simple  Specify a plaintext key

[Comware7-hwtacacs-tacacs-auth]primary authentication 10.0.100.111 key simple ?
  STRING<1-255>  Plaintext key string

[Comware7-hwtacacs-tacacs-auth]primary authentication 10.0.100.111 key simple password ?
  INTEGER<1-65535>   port number, 49 by default
  single-connection  Transmit HWTACACS packets on an open TCP connection
  vpn-instance       Specify a VPN instance
  <cr>
```

```
[Comware7-hwtacacs-tacacs-auth]primary authentication 10.0.100.111 key simple password

[Comware7-hwtacacs-tacacs-auth]primary authorization 10.0.100.111 key simple password

[Comware7-hwtacacs-tacacs-auth]primary accounting 10.0.100.111 key simple password


[Comware7-hwtacacs-tacacs-auth]user-name-format ?
  keep-original   User name unchanged
  with-domain     User name like XXX@XXX
  without-domain  User name like XXX

[Comware7-hwtacacs-tacacs-auth]user-name-format with-domain ?
  <cr>

[Comware7-hwtacacs-tacacs-auth]user-name-format without-domain


[Comware7]domain tacacs

[Comware7-isp-tacacs]?
Isp view commands:
  accounting               Specify accounting scheme
  authentication           Specify authentication scheme
  authorization            Specify authorization scheme
  authorization-attribute  Configure authorization attributes of the domain
  cfd                      Connectivity Fault Detection (CFD) module
  diagnostic-logfile       Diagnostic log file configuration
  display                  Display current system information
  logfile                  Log file configuration
  monitor                  System monitor
  ping                     Ping function
  quit                     Exit from current command view
  return                   Exit to User View
  save                     Save current configuration
  security-logfile         Security log file configuration
  state                    Specify state of domain
  tracert                  Tracert function
  undo                     Cancel current setting

[Comware7-isp-tacacs]authentication ?
  advpn       Specify AAA configuration for ADVPN user
  default     Specify default AAA configuration for all types of users
  ike         Specify AAA configuration for IKE user
  lan-access  Specify AAA configuration for lan-access service
  login       Specify AAA configuration for login user
  portal      Specify AAA configuration for PORTAL user
  ppp         Specify AAA configuration for PPP user
  super       Specify AAA configuration for super user

[Comware7-isp-tacacs]authentication default ?
  hwtacacs-scheme  Specify HWTACACS scheme
  ldap-scheme      Specify LDAP scheme
  local            Specify local scheme
  none             Specify none scheme
  radius-scheme    Specify RADIUS scheme

[Comware7-isp-tacacs]authentication default hwtacacs-scheme ?
  STRING<1-32>  Scheme name

[Comware7-isp-tacacs]authentication default hwtacacs-scheme tacacs-auth ?
  local          Specify local scheme
  none           Specify none scheme
```

```
  radius-scheme  Specify RADIUS scheme
  <cr>

[Comware7-isp-tacacs]authentication default hwtacacs-scheme tacacs-auth

[Comware7-isp-tacacs]authorization default hwtacacs-scheme tacacs-auth

[Comware7-isp-tacacs]accounting default hwtacacs-scheme tacacs-auth


[Comware7]domain default enable tacacs


[Comware7]user-interface aux 0

[Comware7-line-aux0]authentication-mode ?
  none      Login without authentication
  password  Password authentication
  scheme    Authentication use AAA

[Comware7-line-aux0]authentication-mode scheme ?
  <cr>

[Comware7-line-aux0]authentication-mode scheme


[Comware7-line-vty0-63]authentication-mode ?
  none      Login without authentication
  password  Password authentication
  scheme    Authentication use AAA

[Comware7-line-vty0-63]authentication-mode scheme ?
  <cr>

[Comware7-line-vty0-63]authentication-mode scheme


[Comware7]display hwtacacs ?
  scheme  Specify HWTACACS scheme

[Comware7]display hwtacacs scheme ?
  >             Redirect it to a file
  >>            Redirect it to a file in append mode
  STRING<1-32>  HWTACACS scheme name
  |             Matching output
  <cr>

[Comware7]display hwtacacs scheme
Total 1 TACACS schemes

-------------------------------------------------------------------
HWTACACS Scheme Name  : tacacs-auth
  Index : 0
  Primary Auth Server:
    Host name: Not Configured
    IP  : 10.0.100.111    Port: 49     State: Active
    VPN Instance: Not configured
    Single-connection: Disabled
  Primary Author Server:
    Host name: Not Configured
    IP  : 10.0.100.111    Port: 49     State: Active
    VPN Instance: Not configured
    Single-connection: Disabled
```

```
  Primary Acct Server:
    Host name: Not Configured
    IP  : 10.0.100.111    Port: 49     State: Active
    VPN Instance: Not configured
    Single-connection: Disabled

  VPN Instance                          : Not configured
  NAS IP Address                        : Not configured
  Server Quiet Period(minutes)          : 5
  Realtime Accounting Interval(minutes) : 12
  Response Timeout Interval(seconds)    : 5
  Username Format                       : without-domain
-------------------------------------------------------------------
```

Cisco

```
Cisco(config)#tacacs-server ?
  administration    Start tacacs+ deamon handling administrative messages
  attribute         Customize selected tacacs attributes
  cache             AAA auth cache default server group
  directed-request  Allow user to specify tacacs server to use with `@server'
  dns-alias-lookup  Enable IP Domain Name System Alias lookup for TACACS
                    servers
  domain-stripping  Strip the domain from the username
  host              Specify a TACACS server
  key               Set TACACS+ encryption key.
  packet            Modify TACACS+ packet options
  timeout           Time to wait for a TACACS server to reply

Cisco(config)#tacacs-server host ?
  Hostname or A.B.C.D  IP address of TACACS server

Cisco(config)#tacacs-server host 10.0.100.111 ?
  key                per-server encryption key (overrides default)
  nat                To send client's post NAT address to tacacs+ server
  port               TCP port for TACACS+ server (default is 49)
  single-connection  Multiplex all packets over a single tcp connection to
                     server (for CiscoSecure)
  timeout            Time to wait for this TACACS server to reply (overrides
                     default)
  <cr>

Cisco(config)#tacacs-server host 10.0.100.111 key ?
  0     Specifies an UNENCRYPTED key will follow
  7     Specifies HIDDEN key will follow
  LINE  The UNENCRYPTED (cleartext) shared key

Cisco(config)#tacacs-server host 10.0.100.111 key password ?
  <cr>

Cisco(config)#tacacs-server host 10.0.100.111 key password


Cisco(config)#aaa ?
  accounting       Accounting configurations parameters.
  attribute        AAA attribute definitions
  authentication   Authentication configurations parameters.
  authorization    Authorization configurations parameters.
  cache            AAA cache definitions
  configuration    Authorization configuration parameters.
  dnis             Associate certain AAA parameters to a specific DNIS number
  group            AAA group definitions
  local            AAA Local Authen/Authz Method Lists
```

```
  local            AAA Local method options
  max-sessions     Adjust initial hash size for estimated max sessions
  memory           AAA memory parameters
  nas              NAS specific configuration
  new-model        Enable NEW access control commands and functions.(Disables
                   OLD commands.)
  pod              POD processing
  policy           AAA policy parameters
  server           Local AAA server
  service-profile  Service-Profile parameters
  session-id       AAA Session ID
  traceback        Traceback recording
  user             AAA user definitions

Cisco(config)#aaa authentication ?
  arap             Set authentication lists for arap.
  attempts         Set the maximum number of authentication attempts
  banner           Message to use when starting login/authentication.
  dot1x            Set authentication lists for IEEE 802.1x.
  enable           Set authentication list for enable.
  eou              Set authentication lists for EAPoUDP
  fail-message     Message to use for failed login/authentication.
  login            Set authentication lists for logins.
  password-prompt  Text to use when prompting for a password
  ppp              Set authentication lists for ppp.
  sgbp             Set authentication lists for sgbp.
  suppress         Do not send access request for a specific type of user.
  username-prompt  Text to use when prompting for a username

Cisco(config)#aaa authentication login ?
  WORD     Named authentication list (max 31 characters, longer will be
           rejected).
  default  The default authentication list.

Cisco(config)#aaa authentication login default ?
  cache          Use Cached-group
  enable         Use enable password for authentication.
  group          Use Server-group
  krb5           Use Kerberos 5 authentication.
  krb5-telnet    Allow logins only if already authenticated via Kerberos V
                 Telnet.
  line           Use line password for authentication.
  local          Use local username authentication.
  local-case     Use case-sensitive local username authentication.
  none           NO authentication.
  passwd-expiry  enable the login list to provide password aging support

Cisco(config)#aaa authentication login default group ?
  WORD     Server-group name
  ldap     Use list of all LDAP hosts.
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.

Cisco(config)#aaa authentication login default group tacacs+ ?
  cache       Use Cached-group
  enable      Use enable password for authentication.
  group       Use Server-group
  krb5        Use Kerberos 5 authentication.
  line        Use line password for authentication.
  local       Use local username authentication.
  local-case  Use case-sensitive local username authentication.
  none        NO authentication.
  <cr>
```

```
Cisco(config)#aaa authentication login default group tacacs+

Cisco(config)#aaa authentication enable default group tacacs+


Cisco(config)#line vty 0 15

Cisco(config-line)#login ?
  authentication  Authentication parameters.

Cisco(config-line)#login authentication ?
  WORD     Use an authentication list with this name.
  default  Use the default authentication list.

Cisco(config-line)#login authentication default ?
  <cr>

Cisco(config-line)#login authentication default


Cisco#show tacacs

Tacacs+ Server -  public  :
            Server address: 10.0.100.111
               Server port: 49
              Socket opens:          7
             Socket closes:          7
             Socket aborts:          0
             Socket errors:          0
           Socket Timeouts:          0
   Failed Connect Attempts:          0
        Total Packets Sent:         17
        Total Packets Recv:         17
```

b) Privilege Mode

This feature provides a dedicated login at a specific user level, based on the reply the authentication server sends to the switch.

Must execute the basic configuration in the preceeding section first.

ArubaOS-Switch	Comware	Cisco
(Requires special configuration on the TACACS server)	(Requires special configuration on the TACACS server) No additional Comware HWTACACS configuration required to support this option.	(Requires special configuration on the TACACS server)
`ArubaOS-Switch(config)# aaa authentication login privilege-mode`		
		`Cisco(config)#aaa authorization console`
		`Cisco(config)#aaa authorization exec default group tacacs+`

ArubaOS-Switch# show authentication		

ArubaOS-Switch

(Requires special configuration on the TACACS server)

```
ArubaOS-Switch(config)# aaa ?
 accounting            Configure accounting parameters on the switch.
 authentication        Configure authentication parameters on the switch.
 authorization         Configure authorization parameters on the switch.
 port-access           Configure 802.1X (Port Based Network Access), MAC address based
                       network access, or web authentication based network access on the
                       device.
 server-group          Place the RADIUS server into the RADIUS server group.

ArubaOS-Switch(config)# aaa authentication ?
 allow-vlan            Configure authenticator ports to apply VLAN changes immediately.
 console               Configure authentication mechanism used to control access to the
                       switch console.
 disable-username      Bypass the username during authentication while accessing the
                       switch to get Manager or Operator access.
 local-user            Create or remove a local user account.
 lockout-delay         The number of seconds after repeated login failures before a user
                       may again attempt login.
 login                 Specify that switch respects the authentication server's privilege
                       level.
 mac-based             Configure authentication mechanism used to control mac-based port
                       access to the switch.
 num-attempts          The number of login attempts allowed.
 port-access           Configure authentication mechanism used to control access to the
                       network.
 ssh                   Configure authentication mechanism used to control SSH access to
                       the switch.
 telnet                Configure authentication mechanism used to control telnet access
                       to the switch.
 web                   Configure authentication mechanism used to control web access to
                       the switch.
 web-based             Configure authentication mechanism used to control web-based port
                       access to the switch.

ArubaOS-Switch(config)# aaa authentication login ?
 privilege-mode        Specify that switch respects the authentication server's privilege
                       level.

ArubaOS-Switch(config)# aaa authentication login privilege-mode ?
 <cr>

ArubaOS-Switch(config)# aaa authentication login privilege-mode


ArubaOS-Switch# show authentication

 Status and Counters - Authentication Information

  Login Attempts : 3
  Lockout Delay : 0
  Respect Privilege : Enabled
  Bypass Username For Operator and Manager Access : Disabled
```

```
                  | Login      Login        Login
  Access Task     | Primary    Server Group Secondary
  -------------- + ---------- ------------ ----------
  Console         | Tacacs                  Local
  Telnet          | Tacacs                  None
  Port-Access     | Local                   None
  Webui           | Radius     radius       None
  SSH             | Tacacs                  None
  Web-Auth        | ChapRadius radius       None
  MAC-Auth        | ChapRadius radius       None
  SNMP            | Local                   None
  Local-MAC-Auth  | Local                   None
                  | Local                   None

                  | Enable     Enable       Enable
  Access Task     | Primary    Server Group Secondary
  -------------- + ---------- ------------ ----------
  Console         | Tacacs                  Local
  Telnet          | Tacacs                  None
  Webui           | Radius     radius       None
  SSH             | Tacacs                  None
```

Comware

(Requires special configuration on the TACACS server)

No additional Comware HWTACACS configuration required to support this option.

Cisco

(Requires special configuration on the TACACS server)

```
Cisco(config)#aaa ?
  accounting       Accounting configurations parameters.
  attribute        AAA attribute definitions
  authentication   Authentication configurations parameters.
  authorization    Authorization configurations parameters.
  cache            AAA cache definitions
  configuration    Authorization configuration parameters.
  dnis             Associate certain AAA parameters to a specific DNIS number
  group            AAA group definitions
  local            AAA Local Authen/Authz Method Lists
  local            AAA Local method options
  max-sessions     Adjust initial hash size for estimated max sessions
  memory           AAA memory parameters
  nas              NAS specific configuration
  new-model        Enable NEW access control commands and functions.(Disables
                   OLD commands.)
  pod              POD processing
  policy           AAA policy parameters
  server           Local AAA server
  service-profile  Service-Profile parameters
  session-id       AAA Session ID
  traceback        Traceback recording
  user             AAA user definitions

Cisco(config)#aaa authorization ?
  auth-proxy           For Authentication Proxy Services
  cache                For AAA cache configuration
  commands             For exec (shell) commands.
  config-commands      For configuration mode commands.
  configuration        For downloading configurations from AAA server
  console              For enabling console authorization
```

```
  credential-download  For downloading EAP credential from Local/RADIUS/LDAP
  exec                 For starting an exec (shell).
  multicast            For downloading Multicast configurations from an AAA
                       server
  network              For network services. (PPP, SLIP, ARAP)
  policy-if            For diameter policy interface application.
  prepaid              For diameter prepaid services.
  radius-proxy         For proxying radius packets
  reverse-access       For reverse access connections
  subscriber-service   For iEdge subscriber services (VPDN etc)
  template             Enable template authorization

Cisco(config)#aaa authorization console


Cisco(config)#aaa authorization exec ?
  WORD     Named authorization list (max 31 characters, longer will be
           rejected).
  default  The default authorization list.

Cisco(config)#aaa authorization exec default ?
  cache             Use Cached-group
  group             Use server-group.
  if-authenticated  Succeed if user has authenticated.
  krb5-instance     Use Kerberos instance privilege maps.
  local             Use local database.
  none              No authorization (always succeeds).

Cisco(config)#aaa authorization exec default group ?
  WORD     Server-group name
  ldap     Use list of all LDAP hosts.
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.

Cisco(config)#aaa authorization exec default group tacacs+ ?
  cache             Use Cached-group
  group             Use server-group.
  if-authenticated  Succeed if user has authenticated.
  krb5-instance     Use Kerberos instance privilege maps.
  local             Use local database.
  none              No authorization (always succeeds).
  <cr>

Cisco(config)#aaa authorization exec default group tacacs+
```

c) TACACS Accounting

TACACS accounting was started in the **Basic Configuration section A**. These additional options provide specific reporting information to the TACACS server.

Must execute the basic configuration in the preceeding section first.

ArubaOS-Switch	Comware	Cisco
Not an available feature	(Basic support only; no other specific feature support)	`Cisco(config)#aaa accounting exec default start-stop group tacacs+`
		`Cisco(config)#aaa accounting network default start-stop group tacacs+`
		`Cisco(config)#aaa accounting`

		system default start-stop group tacacs+
		Cisco(config)#aaa accounting commands 15 default stop-only group tacacs+
		Cisco#show aaa user all

ArubaOS-Switch

Not an available feature

Comware

(Basic support only; no other specific feature support)

Cisco

```
Cisco(config)#aaa ?
  accounting       Accounting configurations parameters.
  attribute        AAA attribute definitions
  authentication   Authentication configurations parameters.
  authorization    Authorization configurations parameters.
  cache            AAA cache definitions
  configuration    Authorization configuration parameters.
  dnis             Associate certain AAA parameters to a specific DNIS number
  group            AAA group definitions
  local            AAA Local Authen/Authz Method Lists
  local            AAA Local method options
  max-sessions     Adjust initial hash size for estimated max sessions
  memory           AAA memory parameters
  nas              NAS specific configuration
  new-model        Enable NEW access control commands and functions.(Disables
                   OLD commands.)
  pod              POD processing
  policy           AAA policy parameters
  server           Local AAA server
  service-profile  Service-Profile parameters
  session-id       AAA Session ID
  traceback        Traceback recording
  user             AAA user definitions

Cisco(config)#aaa accounting ?
  auth-proxy        For authentication proxy events.
  commands          For exec (shell) commands.
  connection        For outbound connections. (telnet, rlogin)
  delay-start       Delay PPP Network start record until peer IP address is
                    known.
  dot1x             For dot1x sessions.
  exec              For starting an exec (shell).
  gigawords         64 bit interface counters to support Radius attributes 52 &
                    53.
  include           Include attributes in accounting records unconditionally
  jitter            Set jitter parameters for periodic interval
  multicast         For multicast accounting.
  nested            When starting PPP from EXEC, generate NETWORK records
                    before EXEC-STOP record.
  network           For network services. (PPP, SLIP, ARAP)
  redundancy        AAA platform redundancy accounting behavior
  send              Send records to accounting server.
  session-duration  Set the preference for calculating session durations
  suppress          Do not generate accounting records for a specific type of
```

```
                     user.
  system             For system events.
  update             Enable accounting update records.
  vrrs               For VRRS accounting.

Cisco(config)#aaa accounting exec ?
  WORD     Named Accounting list (max 31 characters, longer will be rejected).
  default  The default accounting list.

Cisco(config)#aaa accounting exec default ?
  none        No accounting.
  start-stop  Record start and stop without waiting
  stop-only   Record stop when service terminates.
  <cr>

Cisco(config)#aaa accounting exec default start-stop ?
  broadcast  Use Broadcast for Accounting
  group      Use Server-group

Cisco(config)#aaa accounting exec default start-stop group ?
  WORD     Server-group name
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.

Cisco(config)#aaa accounting exec default start-stop group tacacs+ ?
  group  Use Server-group
  <cr>

Cisco(config)#aaa accounting exec default start-stop group tacacs+

Cisco(config)#aaa accounting network default start-stop group tacacs+

Cisco(config)#aaa accounting system default start-stop group tacacs+

Cisco(config)#aaa accounting commands 15 default stop-only group tacacs+


Cisco#show aaa user all
--------------------------------------------------
Unique id 11 is currently in use.
    Unique id 11 is freed while doing show aaa user.
Debg: No data available
Radi: No data available
Interface:
  TTY Num = -1
  Stop Received = 0
  Byte/Packet Counts till Call Start:
    Start Bytes In = 0             Start Bytes Out = 0
    Start Paks  In = 0             Start Paks  Out = 0
  Byte/Packet Counts till Service Up:
    Pre Bytes In = 0             Pre Bytes Out = 0
    Pre Paks  In = 0             Pre Paks  Out = 0
  Cumulative Byte/Packet Counts :
    Bytes In = 0             Bytes Out = 0
    Paks  In = 0             Paks  Out = 0
  StartTime = 18:05:16 US-Cent Feb 28 1993
Authen: no data
Kerb: No data available
Meth: No data available
```

```
Preauth: No Preauth data.
General: No General data.
PerU: No data available
Service Profile: No Service Profile data.
  ...
```

Chapter 12 Discovery Protocols – LLDP and CDP

This chapter covers the commands required to configure two protocols used to discover devices on the network:

- Link Layer Discovery Protocol (LLDP), an industry standard protocol for device discovery
- Cisco Discovery Protocol (CDP), a Cisco-specific protocol for device discovery.

ArubaOS-Switch and Comware provide limited support for CDP.

In a heterogeneous network, a standard configuration exchange platform ensures that different types of network devices from different vendors can discover one another and exchange configuration for the sake of interoperability and management.

LLDP is defined in IEEE 802.1AB. The protocol operates at the data link layer to exchange device information between directly connected devices. With LLDP, a device sends local device information (including its major functions, management IP address, device ID, and port ID) as TLV (type, length, and value) triplets in LLDP Data Units (LLDPDUs) to other directly connected devices. At the same time, the device stores the device information received in LLDPDUs sent from the LLDP neighbors in a standard management information base (MIB). LLDP enables a network management system to quickly detect and identify Layer 2 network topology changes.

a) LLDP

ArubaOS-Switch	Comware5	Cisco
(Enabled by default, both globally and per port)	(Enabled by default, both globally and per port)	(Not enabled by default)

(if needed)
 	
`ArubaOS-Switch(config)#`
`  lldp run`
	(if needed)
	
	`[Comware5]lldp enable`
	
	`[Comware5]interface g1/0/1`
	
	`[Comware5-GigabitEthernet1/0/1]lldp enable`
		`Cisco(config)#lldp run`

	`[Comware5]display lldp neighbor-information brief`	
`ArubaOS-Switch# show lldp info remote-device`	`[Comware5]display lldp neighbor-information list`	`Cisco#show lldp neighbors`
`ArubaOS-Switch# show lldp info remote-device 1`	`[Comware5]display lldp neighbor-information interface g1/0/1`	`Cisco#show lldp neighbors g1/0/1 detail`
`ArubaOS-Switch(config)# lldp admin-status oobm [txonly | rxonly | tx_rx | disable]`		`Cisco(config)#lldp {med-tlv-select` *`tlv`* `| receive | transmit}`
`ArubaOS-Switch(config)# lldp enable-notification oobm`		`Cisco(config)#lldp run`

ArubaOS-Switch(config)# show lldp config oobm		Cisco(config)#show lldp [entry{*|word }|errors| interface|[Ethernet numbers]| neighbours [Ethernet number]| detail] | traffic]
ArubaOS-Switch(config)# show lldp info local-device oobm		Cisco(config)#show lldp traffic
ArubaOS-Switch(config)# show lldp info remote-device oobm		Cisco(config)#show lldp neighbours
ArubaOS-Switch(config)# show lldp statsoobm		
ArubaOS-Switch (device-profile)# allow-jumbo-frames		Cisco(enable)#set port jumbo
ArubaOS-Switch (device-profile)# no allow-jumbo-frames		Cisco(enable)# set port jumbo <port> disable
	Comware7	
	(Generally enabled by default, both globally and per port. See notes for additional information)	
	(if needed) [Comware7]lldp global enable [Comware7]interface g1/0/1 [Comware7-GigabitEthernet1/0/1]lldp enable	
	[Comware7]display lldp neighbor-information list	
	[Comware7]display lldp neighbor-information interface g1/0/1	
	[Comware7]display lldp neighbor-information interface g1/0/1 verbose	

ArubaOS-Switch

(Enabled by default, both globally and per port)

(if needed)

```
ArubaOS-Switch(config)# lldp
 admin-status           Set the port operational mode.
 auto-ArubaOS-Switch         Configure various parameters related to lldp automatic
                        ArubaOS-Switching.
 config                 Set theTLV parameters to advertise on port.
 enable-notification    Enable or disable notification on port.
 fast-start-count       Set the MED fast-start count in seconds.
 holdtime-multiplier    Set the holdtime multipler.
```

```
 refresh-interval      Set refresh interval/transmit interval in seconds.
 run                   Start or stop LLDP on the device.
 top-change-notify     Enable or disable LLDP MED topology change notification.

ArubaOS-Switch(config)# lldp run ?
 <cr>

ArubaOS-Switch(config)# lldp run


ArubaOS-Switch# show lldp ?
 auto-ArubaOS-Switch        Show LLDP auto-ArubaOS-Switch related info for radio-ports.
 config                Show LLDP configuration information.
 info                  Show LLDP information about the local or remote device.
 stats                 Show LLDP statistics.

ArubaOS-Switch# show lldp info ?
 local-device          Show LLDP local device information.
 remote-device         Show LLDP remote device information.

ArubaOS-Switch# show lldp info remote-device ?
[ethernet] PORT-LIST  Show local or remote device information for the specified ports.
 <cr>

ArubaOS-Switch# show lldp info remote-device

 LLDP Remote Devices Information

  LocalPort | ChassisId                 PortId PortDescr SysName
  --------- + ------------------------- ------ --------- ----------------------
  1         | c0 91 34 83 8d 80         3      3         2520G-1


ArubaOS-Switch# show lldp info remote-device 1

 LLDP Remote Device Information Detail

  Local Port   : 1
  ChassisType  : mac-address
  ChassisId    : c0 91 34 83 8d 80
  PortType     : local
  PortId       : 3
  SysName      : 2520G-1
  System Descr : ProCurve J9299A Switch 2520G-24-PoE, revision J.14.54, RO...
  PortDescr    : 3
  Pvid         :

  System Capabilities Supported  : bridge
  System Capabilities Enabled    : bridge

  Remote Management Address
     Type    : ipv4
     Address : 10.0.111.2
```

Comware5

(Enabled by default, both globally and per port)

(if needed)

```
[Comware5]lldp ?
  compliance       Enable compliance with another link layer discovery protocol
  enable           Enable capability
```

```
  fast-count       The fast-start times of transmitting frames
  hold-multiplier  Hold multiplicator for TTL
  timer            Timer of LLDP

[Comware5]lldp enable ?
  <cr>

[Comware5]lldp enable

[Comware5]interface g1/0/1

[Comware5-GigabitEthernet1/0/1]lldp enable


[Comware5]display lldp ?
  local-information     Display local information
  neighbor-information  Display neighbor information
  statistics            Display statistics information
  status                Display LLDP status and configuration
  tlv-config            Display TLV configuration

[Comware5]display lldp neighbor-information ?
  brief      Brief message
  interface  Specify interface
  list       Neighbor list
  |          Matching output
  <cr>

[Comware5]display lldp neighbor-information brief ?
  |          Matching output
  <cr>

[Comware5]display lldp neighbor-information brief

LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
  Neighbor 1:
  ChassisID/subtype: c091-3483-8d80/MAC address
  PortID/subtype   : 9/Locally assigned
  Capabilities     : Bridge


[Comware5]display lldp neighbor-information list

System Name          Local Interface Chassis ID      Port ID
2520G-1              GE1/0/1         c091-3483-8d80  9


[Comware5]display lldp neighbor-information interface g1/0/1

LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
  Neighbor index   : 1
  Update time      : 0 days,0 hours,1 minutes,26 seconds
  Chassis type     : MAC address
  Chassis ID       : c091-3483-8d80
  Port ID type     : Locally assigned
  Port ID          : 9
  Port description : 9
  System name        : 2520G-1
  System description : ProCurve J9299A Switch 2520G-24-PoE, revision J.14.54, ROM J.14.05
(/sw/code/build/walle(J_t4b))
  System capabilities supported : Bridge
  System capabilities enabled   : Bridge
```

```
  Management address type           : ipv4
  Management address                : 10.0.111.2
  Management address interface type : IfIndex
  Management address interface ID   : Unknown
  Management address OID            : 0

  Auto-negotiation supported : Yes
  Auto-negotiation enabled   : Yes
  OperMau                    : speed(1000)/duplex(Full)
```

Comware7

By default:

- If the switch starts up with empty configuration, LLDP is disabled globally (initial setting).
- If the switch starts up with the default configuration file (also included via the .ipe file), LLDP is enabled globally (factory default).

(Based on above information, generally enabled by default, both globally and per port)

(if needed)

```
[Comware7]lldp ?
  compliance       Enable compliance with another link layer discovery protocol
  fast-count       The fast-start times of transmitting frames
  global           Specify global
  hold-multiplier  Hold multiplicator for TTL
  max-credit       Specify LLDP maximum transmit credit
  mode             Specify LLDP bridge mode
  timer            Timer of LLDP

[Comware7]lldp global ?
  enable  Enable capability

[Comware7]lldp global enable ?
  <cr>

[Comware7]lldp global enable

[Comware7]interface g1/0/1

[Comware7-GigabitEthernet1/0/1]lldp enable


[Comware7]display lldp ?
  local-information     Display local information
  neighbor-information  Display neighbor information
  statistics            Display statistics information
  status                Display LLDP status and configuration
  tlv-config            Display TLV configuration

[Comware7]display lldp neighbor-information ?
  >          Redirect it to a file
  >>         Redirect it to a file in append mode
  agent      Specify LLDP agent
  interface  Specify interface
  list       Neighbor list
  verbose    Verbose message
  |          Matching output
  <cr>

[Comware7]display lldp neighbor-information list
Chassis ID : * -- -- Nearest nontpmr bridge neighbor
```

```
             # -- -- Nearest customer bridge neighbor
             Default -- -- Nearest bridge neighbor
System Name          Local Interface Chassis ID      Port ID
2520G-1              GE1/0/1         c091-3483-8d80  13


[Comware7]display lldp neighbor-information interface g1/0/1 ?
  >        Redirect it to a file
  >>       Redirect it to a file in append mode
  agent    Specify LLDP agent
  verbose  Verbose message
  |        Matching output
  <cr>

[Comware7]display lldp neighbor-information interface g1/0/1
LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 1
 ChassisID/subtype   : c091-3483-8d80/MAC address
 PortID/subtype      : 13/Locally assigned
 Capabilities        : Bridge

[Comware7]display lldp neighbor-information interface g1/0/1 verbose
LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 1
 Update time         : 0 days, 0 hours, 1 minutes, 57 seconds
 Chassis type        : MAC address
 Chassis ID          : c091-3483-8d80
 Port ID type        : Locally assigned
 Port ID             : 13
 Time to live        : 120
 Port description    : 13
 System name         : 2520G-1
 System description  : ProCurve J9299A Switch 2520G-24-PoE, revision J.14.54, RO
                       M J.14.05 (/sw/code/build/walle(J_t4b))
 System capabilities supported : Bridge
 System capabilities enabled   : Bridge
 Management address type           : IPv4
 Management address                : 10.0.111.2
 Management address interface type : IfIndex
 Management address interface ID   : Unknown
 Management address OID            : 0
 Auto-negotiation supported : Yes
 Auto-negotiation enabled   : Yes
 OperMau                    : Speed(1000)/Duplex(Full)
```

Cisco

(Not enabled by default)

```
Cisco(config)#lldp run


Cisco#show lldp ?
  entry      Information for specific neighbor entry
  errors     LLDP computational errors and overflows
  interface  LLDP interface status and configuration
  neighbors  LLDP neighbor entries
  traffic    LLDP statistics
  |          Output modifiers
  <cr>
```

```
Cisco#show lldp neighbors ?
  FastEthernet        FastEthernet IEEE 802.3
  GigabitEthernet     GigabitEthernet IEEE 802.3z
  TenGigabitEthernet  Ten Gigabit Ethernet
  detail              Show detailed information
  |                   Output modifiers
  <cr>

Cisco#show lldp neighbors

Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf     Hold-time  Capability      Port ID
2520G-1             Gi1/0/1        120        B               15

Total entries displayed: 1


Cisco#show lldp neighbors g1/0/1 ?
  detail  Show detailed information
  |       Output modifiers
  <cr>

Cisco#show lldp neighbors g1/0/1
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf     Hold-time  Capability      Port ID
2520G-1             Gi1/0/1        120        B               15

Total entries displayed: 1

Cisco#show lldp neighbors g1/0/1 detail
------------------------------------------------
Chassis id: c091.3483.8d80
Port id: 15
Port Description: 15
System Name: 2520G-1

System Description:
ProCurve J9299A Switch 2520G-24-PoE, revision J.14.54, ROM J.14.05
(/sw/code/build/walle(J_t4b))

Time remaining: 99 seconds
System Capabilities: B
Enabled Capabilities: B
Management Addresses:
    IP: 10.0.111.2
Auto Negotiation - supported, enabled
Physical media capabilities:
    1000baseT(FD)
    100base-TX(FD)
    100base-TX(HD)
    10base-T(FD)
    10base-T(HD)
Media Attachment Unit type: 30
Vlan ID: - not advertised


Total entries displayed: 1
```

b) CDP

ArubaOS-Switch	Comware5	Cisco
(CDP Receive only support enabled by default, both globally and per port)	(CDP compliance mode not enabled by default. Requires LLDP to be enabled)	(Enabled by default, both globally and per port)
(if needed) `ArubaOS-Switch(config)# cdp run`	`[Comware5]lldp compliance cdp`	(if needed) `Cisco(config)#cdp run`
	(enable CDP compliance support on individual ports as needed) `[Comware5-GigabitEthernet1/0/5]lldp compliance admin-status cdp txrx`	
`ArubaOS-Switch# show cdp`		`Cisco#show cdp`
`ArubaOS-Switch# show cdp neighbors`	`[Comware5]display lldp neighbor-information brief`	`Cisco#show cdp neighbors`
`ArubaOS-Switch# show cdp neighbors 5`		`Cisco#show cdp neighbors g1/0/5`
`ArubaOS-Switch# show cdp neighbors 5 detail`	`[Comware5]display lldp neighbor-information interface g1/0/5`	`Cisco#show cdp neighbors g1/0/5 detail`
	Comware7	
	(CDP compliance mode not enabled by default. Requires LLDP to be enabled)	
	`[Comware7]lldp compliance cdp`	
	(enable CDP compliance support on individual ports as needed) `[Comware7-GigabitEthernet1/0/5]lldp compliance admin-status cdp txrx`	
	`[Comware7]display lldp neighbor-information`	
	`[Comware7]display lldp neighbor-information interface g1/0/5 verbose`	

ArubaOS-Switch

(CDP Receive only support enabled by default, both globally and per port)

(if needed)

```
ArubaOS-Switch(config)# cdp ?
 enable                 Enable/disable CDP on particular device ports.
 mode                   Set various modes of CDP (Cisco Discovery Protocol) processing.
 run                    Start and stop CDP on the device.

ArubaOS-Switch(config)# cdp run ?
 <cr>
```

```
ArubaOS-Switch(config)# cdp run


ArubaOS-Switch# show cdp ?
 neighbors             Show CDP neighbors.
 <cr>

ArubaOS-Switch# show cdp

 Global CDP information

  Enable CDP [Yes] : Yes
  CDP mode [rxonly] : rxonly


  Port CDP
  ---- --------
  1    enabled
  2    enabled
  3    enabled
...


ArubaOS-Switch# show cdp neighbors ?
 detail                Show neighbor information field-per-line instead of shortened
                       table format.
 [ethernet] PORT-NUM   Show CDP neighbors on specified port only.
 <cr>

ArubaOS-Switch# show cdp neighbors

 CDP neighbors information

  Port  Device ID                     | Platform                     Capability
  ----- ----------------------------- + ---------------------------- -----------
  1     c0 91 34 83 8d 80             | ProCurve J9299A Switch 25... S
  5     SEP001E7A2542D1               | SCCP41.8-5-2SR1SCisco IP ...
  5     01 0a 00 6f 68                | Cisco IP Phone CP-7961G-G... S

ArubaOS-Switch# show cdp neighbors 5
 detail                Show neighbor information field-per-line instead of shortened
                       table format.
 <cr>

ArubaOS-Switch# show cdp neighbors 5

 CDP neighbors information for port 5

  Port  Device ID                     | Platform                     Capability
  ----- ----------------------------- + ---------------------------- -----------
  5     SEP001E7A2542D1               | SCCP41.8-5-2SR1SCisco IP ...
  5     01 0a 00 6f 68                | Cisco IP Phone CP-7961G-G... S

ArubaOS-Switch# show cdp neighbors 5 detail ?
 <cr>

ArubaOS-Switch# show cdp neighbors 5 detail

 CDP neighbors information for port 5

  Port : 5
  Device ID : SEP001E7A2542D1
```

```
  Address Type : IP
  Address      : 10.0.111.104
  Platform     : SCCP41.8-5-2SR1SCisco IP Phone 7961
  Capability   :
  Device Port  : Port 1
  Version      : SCCP41.8-5-2SR1SCisco IP Phone 7961

--------------------------------------------------------------------------------

  Port : 5
  Device ID : 01 0a 00 6f 68
  Address Type : IP
  Address      : 10.0.111.104
  Platform     : Cisco IP Phone CP-7961G-GE,V2, SCCP41.8-5-2SR1S
  Capability   : Switch
  Device Port  : SW PORT
  Version      : Cisco IP Phone CP-7961G-GE,V2, SCCP41.8-5-2SR1S
```

Comware5

(CDP compliance mode not enabled by default. Requires LLDP to be enabled)

```
[Comware5]lldp ?
  compliance       Enable compliance with another link layer discovery protocol
  enable           Enable capability
  fast-count       The fast-start times of transmitting frames
  hold-multiplier  Hold multiplicator for TTL
  timer            Timer of LLDP

[Comware5]lldp compliance ?
  cdp  Non standard IEEE discovery protocol

[Comware5]lldp compliance cdp ?
  <cr>

[Comware5]lldp compliance cdp


[Comware5-GigabitEthernet1/0/5]lldp ?
  admin-status               Specify transmit/receive mode of LLDP on the port
  check-change-interval      Specify interval of checking system changes
  compliance                 Specify the mode for transmitting/receiving frames
                             of the specified link layer discovery protocol on
                             the port
  enable                     Enable capability
  encapsulation              Specify lldp frame formats
  management-address-format  Specify management-address formats
  management-address-tlv     Management address for other protocol
  notification               Enable the trap capability
  tlv-enable                 Enable optional TLV
  voice-vlan                 Specify voice VLAN

[Comware5-GigabitEthernet1/0/5]lldp compliance ?
  admin-status  Specify the mode for transmitting/receiving frames of the
                specified link layer discovery protocol on the port

[Comware5-GigabitEthernet1/0/5]lldp compliance admin-status ?
  cdp  Non standard IEEE discovery protocol

[Comware5-GigabitEthernet1/0/5]lldp compliance admin-status cdp ?
  disable  Disable transmitting and receiving frames of the specified link
           layer discovery protocol
  txrx     Enable transmitting and receiving frames of the specified link layer
```

```
            discovery protocol

[Comware5-GigabitEthernet1/0/5]lldp compliance admin-status cdp txrx ?
  <cr>

[Comware5-GigabitEthernet1/0/5]lldp compliance admin-status cdp txrx


[Comware5]display lldp ?
  local-information     Display local information
  neighbor-information  Display neighbor information
  statistics            Display statistics information
  status                Display LLDP status and configuration
  tlv-config            Display TLV configuration

[Comware5]display lldp neighbor-information ?
  brief      Brief message
  interface  Specify interface
  list       Neighbor list
  |          Matching output
  <cr>

[Comware5]display lldp neighbor-information brief

LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
  Neighbor 1:
  ChassisID/subtype: c091-3483-8d80/MAC address
  PortID/subtype   : 9/Locally assigned
  Capabilities     : Bridge

CDP neighbor-information of port 5[GigabitEthernet1/0/5]:
  CDP neighbor index : 1
  Chassis ID         : SEP001AA107BD05
  Address            : 10.0.111.101
  Port ID            : Port 1

[Comware5]display lldp neighbor-information interface ?
  GigabitEthernet  GigabitEthernet interface

[Comware5]display lldp neighbor-information interface g1/0/5 ?
  brief  Brief message
  |      Matching output
  <cr>

[Comware5]display lldp neighbor-information interface g1/0/5

CDP neighbor-information of port 5[GigabitEthernet1/0/5]:
  CDP neighbor index : 1
  Chassis ID         : SEP001AA107BD05
  Address            : 10.0.111.101
  Port ID            : Port 1
  Software version   : SIP41.8-2-2SR2S
  Platform           : Cisco IP Phone 7961
  Duplex             : Full
```

Comware7

(CDP compliance mode not enabled by default. Requires LLDP to be enabled)

```
[Comware7]lldp ?
  compliance       Enable compliance with another link layer discovery protocol
  fast-count       The fast-start times of transmitting frames
  global           Specify global
```

```
  hold-multiplier  Hold multiplicator for TTL
  max-credit       Specify LLDP maximum transmit credit
  mode             Specify LLDP bridge mode
  timer            Timer of LLDP

[Comware7]lldp compliance ?
  cdp  Non standard IEEE discovery protocol

[Comware7]lldp compliance cdp ?
  <cr>

[Comware7]lldp compliance cdp


[Comware7-GigabitEthernet1/0/5]lldp ?
  admin-status               Specify transmit/receive mode of LLDP on the port
  agent                      Specify LLDP agent
  check-change-interval      Specify interval of checking system changes
  compliance                 Enable compliance with another link layer discovery
                             protocol
  enable                     Enable capability
  encapsulation              Specify lldp frame formats
  management-address-format  Specify management-address formats
  notification               Enable the trap capability
  tlv-enable                 Enable optional TLV

[Comware7-GigabitEthernet1/0/5]lldp compliance ?
  admin-status  Specify the mode for transmitting/receiving frames of the
                specified link layer discovery protocol on the port

[Comware7-GigabitEthernet1/0/5]lldp compliance admin-status ?
  cdp  Non standard IEEE discovery protocol

[Comware7-GigabitEthernet1/0/5]lldp compliance admin-status cdp ?
  disable  Disable transmitting and receiving frames of the specified link layer
           discovery protocol
  txrx     Enable transmitting and receiving frames of the specified link layer
           discovery protocol

[Comware7-GigabitEthernet1/0/5]lldp compliance admin-status cdp txrx ?
  <cr>

[Comware7-GigabitEthernet1/0/5]lldp compliance admin-status cdp txrx


[Comware7]display lldp ?
  local-information     Display local information
  neighbor-information  Display neighbor information
  statistics            Display statistics information
  status                Display LLDP status and configuration
  tlv-config            Display TLV configuration

[Comware7]display lldp neighbor-information ?
  >          Redirect it to a file
  >>         Redirect it to a file in append mode
  agent      Specify LLDP agent
  interface  Specify interface
  list       Neighbor list
  verbose    Verbose message
  |          Matching output
  <cr>

[Comware7]display lldp neighbor-information
```

```
LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 1
 ChassisID/subtype   : c091-3483-8d80/MAC address
 PortID/subtype      : 13/Locally assigned
 Capabilities        : Bridge

CDP neighbor-information of port 5[GigabitEthernet1/0/5]:
LLDP agent nearest-bridge:
 CDP neighbor index  : 1
 Chassis ID          : SEP0013608622A2
 Port ID             : Port 1

[Comware7]display lldp neighbor-information interface ?
  FortyGigE            FortyGigE interface
  GigabitEthernet      GigabitEthernet interface
  M-GigabitEthernet    MGE interface
  Ten-GigabitEthernet  Ten-GigabitEthernet interface

[Comware7]display lldp neighbor-information interface g1/0/5 ?
  >        Redirect it to a file
  >>       Redirect it to a file in append mode
  agent    Specify LLDP agent
  verbose  Verbose message
  |        Matching output
  <cr>

[Comware7]display lldp neighbor-information interface g1/0/5
CDP neighbor-information of port 5[GigabitEthernet1/0/5]:
LLDP agent nearest-bridge:
 CDP neighbor index  : 1
 Chassis ID          : SEP0013608622A2
 Port ID             : Port 1

[Comware7]display lldp neighbor-information interface g1/0/5 verbose ?
  >     Redirect it to a file
  >>    Redirect it to a file in append mode
  |     Matching output
  <cr>

[Comware7]display lldp neighbor-information interface g1/0/5 verbose
CDP neighbor-information of port 5[GigabitEthernet1/0/5]:
LLDP agent nearest-bridge:
 CDP neighbor index  : 1
 Chassis ID          : SEP0013608622A2
 Addresses           : 10.0.111.102
 Port ID             : Port 1
 Software version    : P00307020400
 Platform version    : Cisco IP Phone 7960
 Duplex              : Full
 Time to live        : 180
```

Cisco

(Enabled by default, both globally and per port)

(if needed)

```
Cisco(config)#cdp ?
  advertise-v2  CDP sends version-2 advertisements
  holdtime      Specify the holdtime (in sec) to be sent in packets
  run           Enable CDP
```

```
  timer         Specify the rate at which CDP packets are sent (in sec)
  tlv           Enable exchange of specific tlv information

Cisco(config)#cdp run ?
  <cr>

Cisco(config)#cdp run


Cisco#show cdp ?
  entry      Information for specific neighbor entry
  interface  CDP interface status and configuration
  neighbors  CDP neighbor entries
  traffic    CDP statistics
  |          Output modifiers
  <cr>

Cisco#show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled

Cisco#show cdp neighbors ?
  Async               Async interface
  Auto-Template       Auto-Template interface
  BVI                 Bridge-Group Virtual Interface
  CTunnel             CTunnel interface
  Dialer              Dialer interface
  FastEthernet        FastEthernet IEEE 802.3
  Filter              Filter interface
  Filtergroup         Filter Group interface
  GigabitEthernet     GigabitEthernet IEEE 802.3z
  GroupVI             Group Virtual interface
  Lex                 Lex interface
  Port-channel        Ethernet Channel of interfaces
  Portgroup           Portgroup interface
  Pos-channel         POS Channel of interfaces
  TenGigabitEthernet  Ten Gigabit Ethernet
  Tunnel              Tunnel interface
  Vif                 PGM Multicast Host interface
  Virtual-Template    Virtual Template interface
  Virtual-TokenRing   Virtual TokenRing
  Vlan                Catalyst Vlans
  detail              Show detailed information
  fcpa                Fiber Channel
  |                   Output modifiers
  <cr>

Cisco#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
SEP001AA133A2FA  Gig 1/0/5         149              H P   IP Phone  Port 1

Cisco#show cdp neighbors g1/0/5 ?
  detail  Show detailed information
  |       Output modifiers
  <cr>

Cisco#show cdp neighbors g1/0/5
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
SEP001AA133A2FA  Gig 1/0/5         132              H P   IP Phone  Port 1


Cisco#show cdp neighbors g1/0/5 detail
-------------------------
Device ID: SEP001AA133A2FA
Entry address(es):
  IP address: 10.0.111.103
Platform: Cisco IP Phone 7961,  Capabilities: Host Phone
Interface: GigabitEthernet1/0/5,  Port ID (outgoing port): Port 1
Holdtime : 140 sec

Version :
SIP41.8-2-2SR2S

advertisement version: 2
Duplex: full
Power drawn: 6.300 Watts
Power request id: 41722, Power management id: 1
Power request levels are:6300 0 0 0 0
Management address(es):
```

Chapter 13 Out-of-Band Management

One of the first key questions about securing a network switch is "Is my management traffic in-band or out-of-band?" The differences can be described as follows:

- In-band – switch management traffic travels with the network data traffic on the data plane and can be impacted when communication problems arise on the data plane
- Out-of-band – switch management traffic travels on a different plane than the network data traffic and is not impacted when communication problems arise on the data plane.

In documentation, it is common to describe "out-of-band" connections as being associated with the Management Plane and "in-band" connections as being associated with the Data Plane.

Management Plane

Serial Console: For the out-of-band, switches supports a serial console allowing a computer or console server to connect. This connection is speed limited and limited to the Command Line Interface. In addition, the serial interface doesn't support other types of management traffic – like RADIUS, SNMP, or Syslog – where the switch is acting like a client.

Out-of-band Management (OOBM) and Management ports generally refer to an Ethernet port that is dedicated to management. A variety of protocols can be supported over the management port based on available features by product/operating system.

Data Plane

A management Virtual Local Area Network (VLAN) is a VLAN with severe network configuration restrictions focused only on switch management.

A loopback interface can be protected using Access Control Lists, and when combined with other security settings, can offer a high degree of security confidence when a management VLAN is too restrictive.

A Data Plane configuration for switch management may be necessary if you need to manage the switch via a Fiber connection since OOBM ports are RJ-45 or if there is no OOBM ports on the switch. In addition, using the Loopback interface method, you can have and control access from multiple VLANs in the network. Of course the downside is that such connections are in the Data Plane and subject to interruption by Data Plane troubles.

ArubaOS-Switch	Comware5	Cisco
`ArubaOS-Switch(config)# oobm`	`Not available`	`Cisco(config)#interface fastEthernet 0`
`ArubaOS-Switch(oobm)# ip address 10.199.111.21/24`		`Cisco(config-if)#ip address 10.199.111.41 255.255.255.0`

ArubaOS-Switch(config)# telnet-server listen oobm		Cisco(config)#ip telnet source-interface fastEthernet 0
ArubaOS-Switch(config)# ip ssh listen oobm		Cisco(config)#ip ssh source-interface fastEthernet 0
ArubaOS-Switch(config)# web-management listen oobm		
ArubaOS-Switch(config)# ntp server 10.199.111.251 oobm		Cisco(config)#ntp source fastEthernet 0
		Cisco(config)#ip tftp source-interface fastEthernet 0
ArubaOS-Switch# ping 10.199.111.51 source oobm		Cisco#ping 10.199.111.21 source fastEthernet 0
ArubaOS-Switch# copy tftp flash 10.199.111.200 KA_16_01_0006.swi primary oobm		Cisco#copy tftp://10.199.111.200/c3750e-universalk9-mz.150-2.SE7.bin flash:/boot/c3750e-universalk9-mz.150-2.SE7.bin
ArubaOS-Switch# show lldp info remote-device oobm		Cisco#show lldp neighbors fastEthernet 0
	Comware7	
	[Comware7]interface M-GigabitEthernet 0/0/0	
	[Comware7-M-GigabitEthernet0/0/0]ip address 10.199.111.51 255.255.255.0	
	[Comware7]telnet client source interface M-GigabitEthernet 0/0/0	
	[Comware7]ssh client source interface M-GigabitEthernet 0/0/0	
	[Comware7]ntp source M-GigabitEthernet 0/0/0	
	[Comware7]ping -i M-GigabitEthernet 0/0/0 10.199.111.41	
	<Comware7>tftp 10.199.111.200 get 5900_5920-CMW710-R2422P01.ipe source interface M-GigabitEthernet 0/0/0	
	<Comware7>display lldp neighbor-information interface M-GigabitEthernet 0/0/0	

ArubaOS-Switch

```
ArubaOS-Switch(config)# oobm
 disable                Disable OOBM.
 enable                 Enable OOBM.
 interface              Configure various interface parameters for OOBM.
 ip                     Configure various IP parameters for the OOBM.
 ipv6                   Configure various IPv6 parameters for the OOBM.
 ntp                    Enable/configure NTP operation on the VLAN/OOBM.
 <cr>
```

```
ArubaOS-Switch(oobm)# ip ?
 address                Set IP parameters for communication within an IP network.
 default-gateway        Configure the IPv4 default gateway address, which will be used
                        when routing is not enabled on the switch.

ArubaOS-Switch(oobm)# ip address ?
 dhcp-bootp             Configure the interface to use DHCP/Bootp server to acquire
                        parameters.
 IP-ADDR/MASK-LENGTH    Interface IP address/mask.

ArubaOS-Switch(oobm)# ip address 10.199.111.21/24 ?
 <cr>
ArubaOS-Switch(oobm)# ip address 10.199.111.21/24

ArubaOS-Switch(oobm)# ip default-gateway ?
 IP-ADDR                IPv4 address of the default gateway.

ArubaOS-Switch(oobm)# ip default-gateway 10.199.111.1 ?
 <cr>
ArubaOS-Switch(oobm)# ip default-gateway 10.199.111.1


ArubaOS-Switch(config)# telnet-server listen ?
 oobm                   Enable Telnet Server on OOBM Interface only.
 data                   Enable Telnet Server on Data Plane only.
 both                   Enable Telnet Server on both OOBM and Data planes.

ArubaOS-Switch(config)# telnet-server listen oobm


ArubaOS-Switch(config)# ip ssh listen ?
 oobm                   Enable SSH on OOBM Interface only.
 data                   Enable SSH on Data Plane only.
 both                   Enable SSH on both OOBM and Data planes.

ArubaOS-Switch(config)# ip ssh listen oobm


ArubaOS-Switch(config)# web-management listen ?
 oobm                   Enable HTTP Server on OOBM Interface only.
 data                   Enable HTTP Server on Data Plane only.
 both                   Enable HTTP Server on both OOBM and Data planes.

ArubaOS-Switch(config)# web-management listen oobm


ArubaOS-Switch(config)# ntp server 10.199.111.251 ?
 burst                  Enables burst mode.
 iburst                 Enables initial burst (iburst) mode.
 key-id                 Set the authentication key to use for this server.
 max-poll               Configures the maximum time intervals in seconds.
 min-poll               Configures the minimum time intervals in seconds.
 oobm                   Use the OOBM interface to connect to the server.
 <cr>

ArubaOS-Switch(config)# ntp server 10.199.111.251 oobm ?
 burst                  Enables burst mode.
 iburst                 Enables initial burst (iburst) mode.
 key-id                 Set the authentication key to use for this server.
 max-poll               Configures the maximum time intervals in seconds.
 min-poll               Configures the minimum time intervals in seconds.
 <cr>
```

```
ArubaOS-Switch(config)# ntp server 10.199.111.251 oobm


ArubaOS-Switch# ping 10.199.111.51 ?
 ip-option             Specify the IP options to use.
 tos                   Specify the Type of Service value to send.
 data-fill             Specify the data pattern to send.
 data-size             Specify the ping data size.
 interval              Specify the interval between pings in seconds.
 repetitions           Ping the device multiple times.
 source                Specify the ping source.
 timeout               Specify the ping timeout in seconds.
 <cr>

ArubaOS-Switch# ping 10.199.111.51 source ?
 IP-ADDR               The source IPv4 address.
 loopback              Specify the source loopback interface.
 oobm                  Use the OOBM interface.
 VLAN-ID               The source VLAN.

ArubaOS-Switch# ping 10.199.111.51 source oobm ?
 data-fill             Specify the data pattern to send.
 data-size             Specify the ping data size.
 interval              Specify the interval between pings in seconds.
 repetitions           Ping the device multiple times.
 timeout               Specify the ping timeout in seconds.
 <cr>

ArubaOS-Switch# ping 10.199.111.51 source oobm
10.199.111.51 is alive, time = 1 ms


ArubaOS-Switch# copy tftp flash 10.199.111.200 KA_16_01_0006.swi primary ?
 oobm                  Use the OOBM interface to reach TFTP server.
 <cr>

ArubaOS-Switch# copy tftp flash 10.199.111.200 KA_16_01_0006.swi primary oobm ?

 <cr>
ArubaOS-Switch# copy tftp flash 10.199.111.200 KA_16_01_0006.swi primary oobm


ArubaOS-Switch# show lldp info remote-device ?
 oobm                  Show local or remote device information for the OOBM port.
 [ethernet] PORT-LIST  Show local or remote device information for the specified ports.
 <cr>

ArubaOS-Switch# show lldp info remote-device oobm ?
 <cr>

ArubaOS-Switch# show lldp info remote-device oobm

 LLDP Remote Device Information Detail

  Local Port   : OOBM
  ChassisType  : mac-address
  ChassisId    : 00 25 61 d7 c5 60
  PortType     : local
  PortId       : 1
  SysName      : 2520-8-OOBM
  System Descr : ProCurve J9137A Switch 2520-8-PoE, revision S.14.03, ROM ...
  PortDescr    : 1
  Pvid         :
```

```
  System Capabilities Supported  : bridge
  System Capabilities Enabled    : bridge

  Remote Management Address
     Type    : ipv4
     Address : 10.199.111.2
```

Comware5

```
Not available
```

Comware7

```
[Comware7]interface M-GigabitEthernet 0/0/0

[Comware7-M-GigabitEthernet0/0/0]?
M-gigabitethernet interface view commands:
  arp                  ARP module
  bandwidth            Specify the expected bandwidth
  bfd                  BFD module
  cfd                  Connectivity Fault Detection (CFD) module
  ddns                 Dynamic Domain Name System (DDNS) module
  default              Restore the default settings
  description          Describe the interface
  dhcp                 Dynamic Host Configuration Protocol (DHCP) commands
  diagnostic-logfile   Diagnostic log file configuration
  display              Display current system information
  duplex               Status of duplex
  ip                   Specify IP configuration
  ipsec                IP Security (IPsec) module
  ipv6                 Specify IPv6 configuration
  isis                 Configure interface parameters for IS-IS
  link-delay           Set the physical state change suppression
  lldp                 Link Layer Discovery Protocol(802.1ab)
  logfile              Log file configuration
  mad                  Multi-active detection
  monitor              System monitor
  mtu                  Specify Maximum Transmission Unit(MTU) of the interface
  ospf                 OSPF interface commands
  ospfv3               OSPFv3 interface commands
  packet-filter        Packet filter settings
  ping                 Ping function
  quit                 Exit from current command view
  return               Exit to User View
  rip                  Configure interface parameters for RIP
  ripng                Configure interface parameters for RIPng
  save                 Save current configuration
  security-logfile     Security log file configuration
  shutdown             Shut down the interface
  speed                Specify speed of current port
  tracert              Tracert function
  undo                 Cancel current setting


[Comware7-M-GigabitEthernet0/0/0]ip ?
  address            Set the IP address of an interface
  binding            Bind the interface with a VPN instance
```

```
  forwarding-table  IP forwarding table
  irdp              Enable the ICMP Router Discovery Protocol

[Comware7-M-GigabitEthernet0/0/0]ip address ?
  X.X.X.X      IP address
  bootp-alloc  Obtain an IP address through BOOTP
  dhcp-alloc   Obtain an IP address through DHCP

[Comware7-M-GigabitEthernet0/0/0]ip address 10.199.111.51 255.255.255.0 ?
  irf-member  Specify an IP address for an IRF member device
  sub         Indicate a subordinate address
  <cr>

[Comware7-M-GigabitEthernet0/0/0]ip address 10.199.111.51 255.255.255.0


[Comware7]telnet ?
  client  Specify telnet client attribute
  server  Telnet server configuration

[Comware7]telnet client ?
  source  Specify a source

[Comware7]telnet client source ?
  interface  Specify a source interface
  ip         Specify a source IP address

[Comware7]telnet client source interface ?
  M-GigabitEthernet  MGE interface
  Vlan-interface     VLAN interface

[Comware7]telnet client source interface M-GigabitEthernet 0/0/0 ?
  <cr>

[Comware7]telnet client source interface M-GigabitEthernet 0/0/0


[Comware7]ssh ?
  client  SSH client configuration
  server  Specify the server attribute
  user    SSH user

[Comware7]ssh client ?
  ipv6    Specify IPv6 protocol
  source  Specify a source address or interface for the SSH client

[Comware7]ssh client source ?
  interface  Specify a source interface
  ip         Specify a source IPv4 address

[Comware7]ssh client source interface ?
  M-GigabitEthernet  MGE interface
  Vlan-interface     VLAN interface

[Comware7]ssh client source interface m
[Comware7]ssh client source interface M-GigabitEthernet 0/0/0 ?
  <cr>

[Comware7]ssh client source interface M-GigabitEthernet 0/0/0


[Comware7]ntp ?
  authentication        Configure NTP authentication
```

```
  authentication-keyid  Specify an authentication key ID
  dscp                  Set the Differentiated Services Codepoint (DSCP) value
  enable                Enable NTP service
  ipv6                  IPv6 protocol
  max-dynamic-sessions  Specify the maximum number of dynamic NTP sessions
  peer                  Permit full access
  query                 Permit control query
  refclock-master       Configure the local clock as a master clock
  reliable              Specify a trusted key
  server                Permit server access and query
  source                Specify a source interface
  synchronization       Permit server access only
  unicast-peer          Specify a NTP peer
  unicast-server        Specify a NTP server

[Comware7]ntp source ?
  M-GigabitEthernet  MGE interface
  Vlan-interface     VLAN interface

[Comware7]ntp source M-GigabitEthernet 0/0/0 ?
  <cr>

[Comware7]ntp source M-GigabitEthernet 0/0/0


[Comware7]ping ?
  -a             Specify the source IP address
  -c             Specify the number of echo requests
  -f             Specify packets not to be fragmented
  -h             Specify the TTL value
  -i             Specify an outgoing interface
  -m             Specify the interval for sending echo requests
  -n             Numeric output only. No attempt will be made to lookup host
                 addresses for symbolic names
  -p             No more than 8 "pad" hexadecimal characters to fill out the
                 sent packet. For example, -p f2 will fill the sent packet with
                 000000f2 repeatedly
  -q             Display only summary
  -r             Record route. Include the RECORD_ROUTE option in the
                 ECHO_REQUEST packets and display the route
  -s             Specify the payload length
  -t             Specify the wait time for each reply
  -tos           Specify the TOS value
  -v             Display the received ICMP packets other than ECHO-RESPONSE
                 packets
  -vpn-instance  Specify a VPN instance
  STRING<1-253>  IP address or hostname of remote system
  ip             IP information
  ipv6           IPv6 information
  mpls           MPLS ping
  trill          TRansparent Interconnection of Lots of Links (TRILL) module

[Comware7]ping -i ?
  M-GigabitEthernet  MGE interface
  Vlan-interface     VLAN interface

[Comware7]ping -i M-GigabitEthernet 0/0/0 ?
  -a             Specify the source IP address
  -c             Specify the number of echo requests
  -f             Specify packets not to be fragmented
  -h             Specify the TTL value
  -m             Specify the interval for sending echo requests
  -n             Numeric output only. No attempt will be made to lookup host
```

```
                  addresses for symbolic names
  -p              No more than 8 "pad" hexadecimal characters to fill out the
                  sent packet. For example, -p f2 will fill the sent packet with
                  000000f2 repeatedly
  -q              Display only summary
  -r              Record route. Include the RECORD_ROUTE option in the
                  ECHO_REQUEST packets and display the route
  -s              Specify the payload length
  -t              Specify the wait time for each reply
  -tos            Specify the TOS value
  -v              Display the received ICMP packets other than ECHO-RESPONSE
                  packets
  -vpn-instance   Specify a VPN instance
  STRING<1-253>   IP address or hostname of remote system

[Comware7]ping -i M-GigabitEthernet 0/0/0 10.199.111.41 ?
  <cr>

[Comware7]ping -i M-GigabitEthernet 0/0/0 10.199.111.41
Ping 10.199.111.41 (10.199.111.41): 56 data bytes, press CTRL_C to break
56 bytes from 10.199.111.41: icmp_seq=0 ttl=255 time=3.488 ms
56 bytes from 10.199.111.41: icmp_seq=1 ttl=255 time=3.065 ms
56 bytes from 10.199.111.41: icmp_seq=2 ttl=255 time=1.773 ms
56 bytes from 10.199.111.41: icmp_seq=3 ttl=255 time=90.936 ms
56 bytes from 10.199.111.41: icmp_seq=4 ttl=255 time=21.390 ms

--- Ping statistics for 10.199.111.41 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.773/24.130/90.936/34.177 ms
[Comware7]%Jun 10 14:42:08:954 2016 Comware7 PING/6/PING_STATIS_INFO: Ping statistics for
10.199.111.41: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip
min/avg/max/std-dev = 1.773/24.130/90.936/34.177 ms.


<Comware7>tftp ?
  STRING<1-253>   IP address or hostname of the TFTP Server
  ipv6            IPv6 TFTP Client

<Comware7>tftp 10.199.111.200 ?
  get   Download a file from the TFTP server
  put   Upload a local file to the TFTP server
  sget  Download a file from the TFTP server securely

<Comware7>tftp 10.199.111.200 get ?
  STRING<1-255>   Source filename

<Comware7>tftp 10.199.111.200 get 5900_5920-CMW710-R2422P01.ipe ?
  STRING<1-255>   Destination filename
  dscp            Set the Differentiated Services Codepoint (DSCP) value
  source          Specify the source address for outgoing TFTP packets
  vpn-instance    Specify a VPN instance
  <cr>

<Comware7>tftp 10.199.111.200 get 5900_5920-CMW710-R2422P01.ipe source ?
  interface  Use the primary address of an interface
  ip         Use a local IP address

<Comware7>tftp 10.199.111.200 get 5900_5920-CMW710-R2422P01.ipe source interface ?
  M-GigabitEthernet  MGE interface
  Vlan-interface     VLAN interface

<Comware7>tftp 10.199.111.200 get 5900_5920-CMW710-R2422P01.ipe source interface
 M-GigabitEthernet 0/0/0 ?
```

```
  dscp  Set the Differentiated Services Codepoint (DSCP) value
  <cr>

<Comware7>tftp 10.199.111.200 get 5900_5920-CMW710-R2422P01.ipe source interface
 M-GigabitEthernet 0/0/0


<Comware7>display lldp ?
  local-information     Display local information
  neighbor-information  Display neighbor information
  statistics            Display statistics information
  status                Display LLDP status and configuration
  tlv-config            Display TLV configuration

<Comware7>display lldp neighbor-information ?
  >          Redirect it to a file
  >>         Redirect it to a file in append mode
  agent      Specify LLDP agent
  interface  Specify interface
  list       Neighbor list
  verbose    Verbose message
  |          Matching output
  <cr>

<Comware7>display lldp neighbor-information interface ?
  FortyGigE            FortyGigE interface
  GigabitEthernet      GigabitEthernet interface
  M-GigabitEthernet    MGE interface
  Ten-GigabitEthernet  Ten-GigabitEthernet interface

<Comware7>display lldp neighbor-information interface M-GigabitEthernet 0/0/0 ?
  >        Redirect it to a file
  >>       Redirect it to a file in append mode
  agent    Specify LLDP agent
  verbose  Verbose message
  |        Matching output
  <cr>

<Comware7>display lldp neighbor-information interface M-GigabitEthernet 0/0/0
LLDP neighbor-information of port 26446[M-GigabitEthernet0/0/0]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 1
 ChassisID/subtype   : 0025-61d7-c560/MAC address
 PortID/subtype      : 6/Locally assigned
 Capabilities        : Bridge
```

Cisco

```
Cisco(config)#interface fastEthernet 0

Cisco(config-if)#?
Interface configuration commands:
  aaa                     Authentication, Authorization and Accounting.
  access-expression       Build a bridge boolean access expression
  arp                     Set arp type (arpa, probe, snap) or timeout or log
                          options
  bandwidth               Set bandwidth informational parameter
  bgp-policy              Apply policy propagated by bgp community string
  carrier-delay           Specify delay for interface transitions
  cdp                     CDP interface subcommands
  clns                    CLNS interface subcommands
  crypto                  Encryption/Decryption commands
```

```
  cts                       Configure Cisco Trusted Security
  dampening                 Enable event dampening
  datalink                  Interface Datalink commands
  default                   Set a command to its defaults
  delay                     Specify interface throughput delay
  description               Interface specific description
  duplex                    Configure duplex operation.
  eou                       EAPoUDP Interface Configuration Commands
  exit                      Exit from interface configuration mode
  flow-sampler              Attach flow sampler to the interface
  flowcontrol               Configure flow operation.
  glbp                      Gateway Load Balancing Protocol interface commands
  help                      Description of the interactive help system
  history                   Interface history histograms - 60 second, 60 minute
                            and 72 hour
  hold-queue                Set hold queue depth
  ip                        Interface Internet Protocol config commands
  ipv6                      IPv6 interface subcommands
  isis                      IS-IS commands
  iso-igrp                  ISO-IGRP interface subcommands
  keepalive                 Enable keepalive
  link                      Configure Link
  lldp                      LLDP interface subcommands
  load-interval             Specify interval for load calculation for an
                            interface
  location                  Interface location information
  logging                   Configure logging for interface
  loopback                  Configure internal loopback on an interface
  macro                     Command macro
  max-reserved-bandwidth    Maximum Reservable Bandwidth on an Interface
  mka                       MACsec Key Agreement (MKA) interface configuration
  neighbor                  interface neighbor configuration mode commands
  network-policy            Network Policy
  nmsp                      NMSP interface configuration
  no                        Negate a command or set its defaults
  ntp                       Configure NTP
  pagp                      PAgP interface subcommands
  power                     Power configuration
  rate-limit                Rate Limit
  routing                   Per-interface routing configuration
  service-policy            Configure CPL Service Policy
  shutdown                  Shutdown the selected interface
  small-frame               Set rate limit parameters for small frame
  snmp                      Modify SNMP interface parameters
  source                    Get config from another source
  spanning-tree             Spanning Tree Subsystem
  speed                     Configure speed operation.
  standby                   HSRP interface configuration commands
  timeout                   Define timeout values for this interface
  topology                  Configure routing topology on the interface
  traffic-shape             Enable Traffic Shaping on an Interface or
                            Sub-Interface
  transmit-interface        Assign a transmit interface to a receive-only
                            interface
  tx-ring-limit             Configure PA level transmit ring limit
  vrf                       VPN Routing/Forwarding parameters on the interface
  vrrp                      VRRP Interface configuration commands
  vtp                       Enable VTP on this interface

Cisco(config-if)#ip ?
Interface IP configuration subcommands:
  access-group        Specify access control for packets
  accounting          Enable IP accounting on this interface
```

```
  address              Set the IP address of an interface
  admission            Apply Network Admission Control
  auth-proxy           Apply authenticaton proxy
  authentication       authentication subcommands
  bandwidth-percent    Set EIGRP bandwidth limit
  bgp                  BGP interface commands
  broadcast-address    Set the broadcast address of an interface
  cef                  Cisco Express Forwarding interface commands
  cgmp                 Enable/disable CGMP
  dampening-change     Percent interface metric must change to cause update
  dampening-interval   Time in seconds to check interface metrics
  dhcp                 Configure DHCP parameters for this interface
  directed-broadcast   Enable forwarding of directed broadcasts
  flow                 NetFlow related commands
  header-compression   IPHC options
  hello-interval       Configures EIGRP-IPv4 hello interval
  helper-address       Specify a destination address for UDP broadcasts
  hold-time            Configures EIGRP-IPv4 hold time
  igmp                 IGMP interface commands
  information-reply    Enable sending ICMP Information Reply messages
  irdp                 ICMP Router Discovery Protocol
  load-sharing         Style of load sharing
  local-proxy-arp      Enable local-proxy ARP
  mask-reply           Enable sending ICMP Mask Reply messages
  mrm                  Configure IP Multicast Routing Monitor tester
  mroute-cache         Enable switching cache for incoming multicast packets
  mtu                  Set IP Maximum Transmission Unit
  multicast            IP multicast interface commands
  next-hop-self        Configures EIGRP-IPv4 next-hop-self
  ospf                 OSPF interface commands
  pim                  PIM interface commands
  policy               Enable policy routing
  probe                Enable HP Probe support
  proxy-arp            Enable proxy ARP
  rarp-server          Enable RARP server for static arp entries
  redirects            Enable sending ICMP Redirect messages
  rgmp                 Enable/disable RGMP
  rip                  Router Information Protocol
  route-cache          Enable fast-switching cache for outgoing packets
  router               IP router interface commands
  rsvp                 RSVP Interface Commands
  rtp                  RTP parameters
  sap                  Session Advertisement Protocol interface commands
  security             DDN IP Security Option
  split-horizon        Perform split horizon
  sticky-arp           Allow the creation of sticky ARP entries
  summary-address      Perform address summarization
  tcp                  TCP interface commands
  unnumbered           Enable IP processing without an explicit address
  unreachables         Enable sending ICMP Unreachable messages
  urd                  Configure URL Rendezvousing
  verify               Enable per packet validation
  vrf                  VPN Routing/Forwarding parameters on the interface
  wccp                 WCCP interface commands

Cisco(config-if)#ip address ?
  A.B.C.D  IP address
  dhcp     IP Address negotiated via DHCP
  pool     IP Address autoconfigured from a local DHCP pool

Cisco(config-if)#ip address 10.199.111.41 255.255.255.0 ?
  secondary  Make this IP address a secondary address
  <cr>
```

```
Cisco(config-if)#ip address 10.199.111.41 255.255.255.0


Cisco(config)#ip telnet ?
  comport           Specify RFC 2217 options
  hidden            Don't display telnet addresses or hostnames
  quiet             Don't display non-error telnet messages
  source-interface  Specify source interface
  tos               Specify type of service

Cisco(config)#ip telnet source-interface ?
  Async               Async interface
  Auto-Template       Auto-Template interface
  BVI                 Bridge-Group Virtual Interface
  CTunnel             CTunnel interface
  Dialer              Dialer interface
  FastEthernet        FastEthernet IEEE 802.3
  Filter              Filter interface
  Filtergroup         Filter Group interface
  GigabitEthernet     GigabitEthernet IEEE 802.3z
  GroupVI             Group Virtual interface
  Lex                 Lex interface
  Loopback            Loopback interface
  Null                Null interface
  Port-channel        Ethernet Channel of interfaces
  Portgroup           Portgroup interface
  Pos-channel         POS Channel of interfaces
  TenGigabitEthernet  Ten Gigabit Ethernet
  Tunnel              Tunnel interface
  Vif                 PGM Multicast Host interface
  Virtual-Template    Virtual Template interface
  Virtual-TokenRing   Virtual TokenRing
  Vlan                Catalyst Vlans
  fcpa                Fiber Channel

Cisco(config)#ip telnet source-interface fastEthernet 0 ?
  <cr>

Cisco(config)#ip telnet source-interface fastEthernet 0


Cisco(config)#ip ssh ?
  authentication-retries  Specify number of authentication retries
  break-string            break-string
  dh                      Diffie-Hellman
  dscp                    IP DSCP value for SSH traffic
  logging                 Configure logging for SSH
  maxstartups             Maximum concurrent sessions allowed
  port                    Starting (or only) Port number to listen on
  precedence              IP Precedence value for SSH traffic
  pubkey-chain            pubkey-chain
  rekey                   Configure rekey values
  rsa                     Configure RSA keypair name for SSH
  source-interface        Specify interface for source address in SSH
                          connections
  stricthostkeycheck      Enable SSH Server Authentication
  time-out                Specify SSH time-out interval
  version                 Specify protocol version to be supported

Cisco(config)#ip ssh source-interface ?
  Async               Async interface
  Auto-Template       Auto-Template interface
```

```
  BVI                  Bridge-Group Virtual Interface
  CTunnel              CTunnel interface
  Dialer               Dialer interface
  FastEthernet         FastEthernet IEEE 802.3
  Filter               Filter interface
  Filtergroup          Filter Group interface
  GigabitEthernet      GigabitEthernet IEEE 802.3z
  GroupVI              Group Virtual interface
  Lex                  Lex interface
  Loopback             Loopback interface
  Null                 Null interface
  Port-channel         Ethernet Channel of interfaces
  Portgroup            Portgroup interface
  Pos-channel          POS Channel of interfaces
  TenGigabitEthernet   Ten Gigabit Ethernet
  Tunnel               Tunnel interface
  Vif                  PGM Multicast Host interface
  Virtual-Template     Virtual Template interface
  Virtual-TokenRing    Virtual TokenRing
  Vlan                 Catalyst Vlans
  fcpa                 Fiber Channel

Cisco(config)#ip ssh source-interface fastEthernet 0 ?
  <cr>

Cisco(config)#ip ssh source-interface fastEthernet 0


Cisco(config)#ntp source ?
  Async                Async interface
  Auto-Template        Auto-Template interface
  BVI                  Bridge-Group Virtual Interface
  CTunnel              CTunnel interface
  Dialer               Dialer interface
  FastEthernet         FastEthernet IEEE 802.3
  Filter               Filter interface
  Filtergroup          Filter Group interface
  GigabitEthernet      GigabitEthernet IEEE 802.3z
  GroupVI              Group Virtual interface
  Lex                  Lex interface
  Loopback             Loopback interface
  Null                 Null interface
  Port-channel         Ethernet Channel of interfaces
  Portgroup            Portgroup interface
  Pos-channel          POS Channel of interfaces
  TenGigabitEthernet   Ten Gigabit Ethernet
  Tunnel               Tunnel interface
  Vif                  PGM Multicast Host interface
  Virtual-Template     Virtual Template interface
  Virtual-TokenRing    Virtual TokenRing
  Vlan                 Catalyst Vlans
  fcpa                 Fiber Channel

Cisco(config)#ntp source fastEthernet 0 ?
  <cr>

Cisco(config)#ntp source fastEthernet 0


Cisco(config)#ip tftp source-interface ?
  Async                Async interface
  Auto-Template        Auto-Template interface
  BVI                  Bridge-Group Virtual Interface
```

```
  CTunnel              CTunnel interface
  Dialer               Dialer interface
  FastEthernet         FastEthernet IEEE 802.3
  Filter               Filter interface
  Filtergroup          Filter Group interface
  GigabitEthernet      GigabitEthernet IEEE 802.3z
  GroupVI              Group Virtual interface
  Lex                  Lex interface
  Loopback             Loopback interface
  Null                 Null interface
  Port-channel         Ethernet Channel of interfaces
  Portgroup            Portgroup interface
  Pos-channel          POS Channel of interfaces
  TenGigabitEthernet   Ten Gigabit Ethernet
  Tunnel               Tunnel interface
  Vif                  PGM Multicast Host interface
  Virtual-Template     Virtual Template interface
  Virtual-TokenRing    Virtual TokenRing
  Vlan                 Catalyst Vlans
  fcpa                 Fiber Channel

Cisco(config)#ip tftp source-interface fastEthernet 0 ?
  <cr>

Cisco(config)#ip tftp source-interface fastEthernet 0


Cisco#ping ?
  WORD  Ping destination address or hostname
  clns  CLNS echo
  ip    IP echo
  ipv6  IPv6 echo
  tag   Tag encapsulated IP echo
  <cr>

Cisco#ping 10.199.111.21 ?
  data      specify data pattern
  df-bit    enable do not fragment bit in IP header
  repeat    specify repeat count
  size      specify datagram size
  source    specify source address or name
  timeout   specify timeout interval
  validate  validate reply data
  <cr>

Cisco#ping 10.199.111.21 source ?
  A.B.C.D              Source address
  Async                Async interface
  Auto-Template        Auto-Template interface
  BVI                  Bridge-Group Virtual Interface
  CTunnel              CTunnel interface
  Dialer               Dialer interface
  FastEthernet         FastEthernet IEEE 802.3
  Filter               Filter interface
  Filtergroup          Filter Group interface
  GigabitEthernet      GigabitEthernet IEEE 802.3z
  GroupVI              Group Virtual interface
  Lex                  Lex interface
  Loopback             Loopback interface
  Null                 Null interface
  Port-channel         Ethernet Channel of interfaces
  Portgroup            Portgroup interface
  Pos-channel          POS Channel of interfaces
```

```
  TenGigabitEthernet  Ten Gigabit Ethernet
  Tunnel              Tunnel interface
  Vif                 PGM Multicast Host interface
  Virtual-Template    Virtual Template interface
  Virtual-TokenRing   Virtual TokenRing
  Vlan                Catalyst Vlans
  fcpa                Fiber Channel

Cisco#ping 10.199.111.21 source fastEthernet 0 ?
  data      specify data pattern
  df-bit    enable do not fragment bit in IP header
  repeat    specify repeat count
  size      specify datagram size
  timeout   specify timeout interval
  validate  validate reply data
  <cr>

Cisco#ping 10.199.111.21 source fastEthernet 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.199.111.21, timeout is 2 seconds:
Packet sent with a source address of 10.199.111.41
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms


Cisco#copy tftp:?
  tftp:  A URL beginning with this prefix

Cisco#copy tftp://10.199.111.200/c3750e-universalk9-mz.150-2.SE7.bin ?
  flash1:         Copy to flash1: file system
  flash:          Copy to flash: file system
  null:           Copy to null: file system
  nvram:          Copy to nvram: file system
  running-config  Update (merge with) current system configuration
  startup-config  Copy to startup configuration
  syslog:         Copy to syslog: file system
  system:         Copy to system: file system
  tmpsys:         Copy to tmpsys: file system

Cisco#copy tftp://10.199.111.200/c3750e-universalk9-mz.150-2.SE7.bin flash:/boot/c3750e-
universalk9-mz.150-2.SE7.bin
Destination filename [/boot/c3750e-universalk9-mz.150-2.SE7.bin]?
Accessing tftp://10.199.111.200/c3750e-universalk9-mz.150-2.SE7.bin...
Loading c3750e-universalk9-mz.150-2.SE7.bin from 10.199.111.200 (via FastEthernet0):


Cisco#show lldp neighbors ?
  FastEthernet        FastEthernet IEEE 802.3
  GigabitEthernet     GigabitEthernet IEEE 802.3z
  TenGigabitEthernet  Ten Gigabit Ethernet
  detail              Show detailed information
  |                   Output modifiers
  <cr>

Cisco#show lldp neighbors fastEthernet 0 ?
  detail  Show detailed information
  |       Output modifiers
  <cr>

Cisco#show lldp neighbors fastEthernet 0
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
```

```
Device ID           Local Intf     Hold-time  Capability      Port ID
2520-8-OOBM         Fa0            98         B               7

Total entries displayed: 1
```

Chapter 14 Job Schedule

Job Schedule enables the user to schedule commands or jobs on the switch for one time or multiple times. This is similar in concept to the UNIX 'cron' utility. The user can schedule any CLI command that the user would otherwise enter interactively. This includes commands to enable or disable ports, LEDs, and Power-Over-Ethernet. Jobs can also be scheduled to be triggered by certain pre-defined events such as switch reboot. The only major restriction on commands scheduled is that, it should not prompt/ask for any user inputs.

ArubaOS-Switch	Comware5	Cisco
ArubaOS-Switch(config)# job save-config at 01:00 "copy run tftp 10.0.100.111 ArubaOS-Switch.cfg"	[Comware5]job save-config	Cisco(config)#file prompt quiet
	[Comware5-job-save-config]view monitor	Cisco(config)#kron policy-list save-config
	[Comware5-job-save-config]time 1 one-off at 02:07 command tftp 10.0.100.111 put startup.cfg	Cisco(config-kron-policy)#cli copy run tftp://10.0.100.111/cisco-startup.cfg
		Cisco(config)#kron occurrence saveconfig at 09:30 oneshot
		Cisco(config-kron-occurrence)#policy-list save-config
ArubaOS-Switch# show job	[Comware5]display job	Cisco(config)#show scheduler config
ArubaOS-Switch# show job save-config	[Comware5]display job save-config	Cisco#show kron schedule
ArubaOS-Switch(config)#job <Name> at [HH:]MM [on <Weekday-List>] [config-save] <Command>		Cisco(config)#scheduler schedule name string
ArubaOS-Switch(config)#job <Name> at [HH:]MM [on [MM/]DD] [config-save] <Command>		Cisco(config)#job name string
ArubaOS-Switch(config)#job <Name> at <Event> [config-save] <Command>		Cisco(config)#time daily time time weekly[[dow:] HH:]MM time monthly [[dm:] HH:] MM time start {now repeat repeat-interval | delta-time [repeat repeat-interval]
ArubaOS-Switch(config)#show job [<Name>]		Cisco(config)#show scheduler schedule [name]
	Comware7	
	[Comware7]scheduler job save-config	
	[Comware7-job-save-config]command 1 tftp 10.0.100.111 put startup.cfg	
	[Comware7]scheduler schedule saveconfig	

	[Comware7-schedule-saveconfig]time once at 01:45	
	[Comware7-schedule-saveconfig]job save-config	
	[Comware7]display scheduler job	
	[Comware7]display scheduler schedule	

ArubaOS-Switch

```
ArubaOS-Switch(config)# job ?
 JOB-NAME-STR          The name of the job to add or delete.

ArubaOS-Switch(config)# job save-config ?
 at                    Schedule when the job runs.
 delay                 Specify the delay before running the job.
 disable               Disable a job.
 enable                Enable a job that is disabled or expired.

ArubaOS-Switch(config)# job save-config at ?
 reboot                Run the job as soon as possible after every switch boot.
 failover              Run the job as soon as possible after standby failover.
 [HH:]MM               The time when the job should run.

ArubaOS-Switch(config)# job save-config at 01:00 ?
 COMMAND-STR           The command to execute when this job runs. Use quotes for
                       multi-word commands.
 config-save           Save configuration changes made by the job.
 on                    Schedule the job to run on specified days.

ArubaOS-Switch(config)# job save-config at 01:00 "copy run tftp 10.0.100.111 ArubaOS-
Switch.cfg" ?
 count                 Specify the number of times the job should run.
 <cr>

ArubaOS-Switch(config)# job save-config at 01:00 "copy run tftp 10.0.100.111 ArubaOS-
Switch.cfg"



ArubaOS-Switch# show job ?
 JOB-NAME-STR          A job name to show additional detail about.
 <cr>

ArubaOS-Switch# show job

 Job Scheduler Status and Configuration

  Scheduler Status : Running

                     Event or             Repeat Save
  Name               Time                 Count  Cfg  Command
  ------------------ -------------------- ------ ---- -------------------------
  save-config        01:00                --     No   copy run tftp 10.0.100.111 provi...

ArubaOS-Switch# show job save-config

 Job Information
```

```
  Job Name    : save-config
  Runs At     : 01:00
  Config Save : No
  Repeat Count: --
  Job Status  : Enabled
  Run Count   : 0
  Error Count : 0
  Command     : copy run tftp 10.0.100.111 ArubaOS-Switch.cfg
```

Comware5

```
[Comware5]job ?
  STRING<1-32>  Name of the task

[Comware5]job save-config ?
  <cr>

[Comware5]job save-config

[Comware5-job-save-config]?
Job view commands:
  cfd       Connectivity fault detection (IEEE 802.1ag)
  display   Display current system information
  mtracert  Trace route to multicast source
  ping      Ping function
  quit      Exit from current command view
  return    Exit to User View
  save      Save current configuration
  time      Execute the scheduled command at the specified time
  tracert   Trace route function
  undo      Undo Command Group
  view      Specify the command view for the task

[Comware5-job-save-config]view ?
  STRING<1-90>  Name of the command view

[Comware5-job-save-config]view monitor ?
  <cr>

[Comware5-job-save-config]view monitor

[Comware5-job-save-config]time ?
  INTEGER<1-10>  The identifier of time

[Comware5-job-save-config]time 1 ?
  at         Specify the exact time
  one-off    Execute the specified command only once
  repeating  Execute a specified command periodically

[Comware5-job-save-config]time 1 one-off ?
  at     Specify the exact time
  delay  Specifies the execution waiting time of a specified command

[Comware5-job-save-config]time 1 one-off at 02:07 ?
  command     Specify the scheduled command
  month-date  Specify the day of the month
  week-day    Specify the day(s) of the week

[Comware5-job-save-config]time 1 one-off at 02:07 command ?
  TEXT  The scheduled command
```

```
[Comware5-job-save-config]time 1 one-off at 02:07 command tftp 10.0.100.111 put startup.cfg
?
   TEXT
   <cr>

[Comware5-job-save-config]time 1 one-off at 02:07 command tftp 10.0.100.111 put startup.cfg



[Comware5]display job ?
  STRING<1-32>  Name of the task
  |             Matching output
  <cr>

[Comware5]display job save-config
Job name: save-config
  Specified view: monitor
  Time 1: Execute command tftp 10.0.100.111 put startup.cfg  at 02:07 today or tomorrow

[Comware5]display job save-config
Job name: save-config
  Specified view: monitor
  Time 1: Execute command tftp 10.0.100.111 put startup.cfg  at 02:07 today or tomorrow has
been executed
```

Comware7

```
[Comware7]scheduler ?
  job       Define a job
  logfile   Scheduler log file configuration
  schedule  Define a schedule

[Comware7]scheduler job ?
  STRING<1-47>  Name of the job

[Comware7]scheduler job save-config ?
  <cr>

[Comware7]scheduler job save-config

[Comware7-job-save-config]?
Job view commands:
  cfd                 Connectivity Fault Detection (CFD) module
  command             Specify a command
  diagnostic-logfile  Diagnostic log file configuration
  display             Display current system information
  ip                  Specify IP configuration
  logfile             Log file configuration
  monitor             System monitor
  ping                Ping function
  quit                Exit from current command view
  return              Exit to User View
  save                Save current configuration
  security-logfile    Security log file configuration
  tracert             Tracert function
  undo                Cancel current setting

[Comware7-job-save-config]command ?
  INTEGER<0-4294967295>  ID of command
```

```
[Comware7-job-save-config]command 1 ?
  TEXT  Command of the job

[Comware7-job-save-config]command 1 tftp 10.0.100.111 put startup.cfg ?
  TEXT  Command of the job
  <cr>

[Comware7-job-save-config]command 1 tftp 10.0.100.111 put startup.cfg

[Comware7-job-save-config]quit

[Comware7]scheduler schedule ?
  STRING<1-47>  Name of the schedule

[Comware7]scheduler schedule saveconfig ?
  <cr>

[Comware7]scheduler schedule saveconfig

[Comware7-schedule-saveconfig]?
Schedule view commands:
  cfd                 Connectivity Fault Detection (CFD) module
  diagnostic-logfile  Diagnostic log file configuration
  display             Display current system information
  ip                  Specify IP configuration
  job                 Assign a job to the schedule
  logfile             Log file configuration
  monitor             System monitor
  ping                Ping function
  quit                Exit from current command view
  return              Exit to User View
  save                Save current configuration
  security-logfile    Security log file configuration
  time                Specify the time to run the schedule
  tracert             Tracert function
  undo                Cancel current setting
  user-role           Specify the user role for executing the schedule

[Comware7-schedule-saveconfig]time ?
  at         Specify the execution time
  once       Run the schedule for once
  repeating  Run the schedule repeatedly

[Comware7-schedule-saveconfig]time once ?
  at     Specify the execution time
  delay  Specify the delay time

[Comware7-schedule-saveconfig]time once at ?
  TIME  Execution time (HH:MM)

[Comware7-schedule-saveconfig]time once at 01:45 ?
  month-date  Specify the day of the month
  week-day    Specify the days of the week
  <cr>

[Comware7-schedule-saveconfig]time once at 01:45

[Comware7-schedule-saveconfig]job ?
  STRING<1-47>  Name of the job

[Comware7-schedule-saveconfig]job save-config ?
  <cr>
```

```
[Comware7-schedule-saveconfig]job save-config



[Comware7]display scheduler ?
  job       Display job information
  logfile   Display scheduler logs
  reboot    Display the reboot time
  schedule  Display schedule information

[Comware7]display scheduler job ?
  >             Redirect it to a file
  >>            Redirect it to a file in append mode
  STRING<1-47>  Name of the job
  |             Matching output
  <cr>

[Comware7]display scheduler job
Job name: save-config
 tftp 10.0.100.111 put startup.cfg

[Comware7]display scheduler schedule ?
  >             Redirect it to a file
  >>            Redirect it to a file in append mode
  STRING<1-47>  Name of the schedule
  |             Matching output
  <cr>

[Comware7]display scheduler schedule
Schedule name        : saveconfig
Schedule type        : Run on Sun Jun 26 01:45:00 2016
Start time           : Sun Jun 26 01:45:00 2016
Last execution time  : Yet to be executed
---------------------------------------------------------------------------
Job name                                          Last execution status
save-config                                       -NA-

[Comware7]display scheduler schedule
Schedule name        : saveconfig
Schedule type        : Run on Sun Jun 26 01:45:00 2016
Start time           : Sun Jun 26 01:45:00 2016
Last execution time  : Sun Jun 26 01:45:00 2016
Last completion time : Sun Jun 26 01:45:06 2016
Execution counts     : 1
---------------------------------------------------------------------------
Job name                                          Last execution status
save-config                                       Successful
```

Cisco

```
Cisco(config)#file ?
  prompt       Prompt level for file operations
  scripts-url  URL to store scripts.
  verify       Verify compressed IOS image checksum

Cisco(config)#file prompt ?
  alert  Prompt only for destructive file operations
  noisy  Confirm all file operation parameters
  quiet  Seldom prompt for file operations
  <cr>
```

```
Cisco(config)#file prompt quiet ?
  <cr>

Cisco(config)#file prompt quiet


Cisco(config)#kron ?
  occurrence   Define the name, time, interval of kron occurrence
  policy-list  Define the name and type of policy-list

Cisco(config)#kron policy-list ?
  WORD  Name of the policy-list being defined

Cisco(config)#kron policy-list save-config ?
  conditional  Execution of the list of cli will stop on failure return values
  <cr>

Cisco(config)#kron policy-list save-config

Cisco(config-kron-policy)#?
KRON Specific commands for this Policy:
  cli   Specify the exec level cli to be executed
  exit  Exit from kron submode
  no    Remove a CLI from the list

Cisco(config-kron-policy)#cli ?
  LINE  Exec level cli to be executed

Cisco(config-kron-policy)#cli copy run tftp://10.0.100.111/cisco-startup.cfg ?
LINE    <cr>

Cisco(config-kron-policy)#cli copy run tftp://10.0.100.111/cisco-startup.cfg

Cisco(config-kron-policy)#exit

Cisco(config)#kron occurrence ?
  WORD  The name of this occurrence

Cisco(config)#kron occurrence saveconfig ?
  at  Date of kron occurrence eg. 14:30 Feb 13
  in  Delta time to kron occurrence

Cisco(config)#kron occurrence saveconfig at ?
  hh:mm  Time of day for occurrence (hh:min eg. 14:30)

Cisco(config)#kron occurrence saveconfig at 09:30 ?
  <1-31>     Day of month
  DAY        Day of Week eg mon, tue, etc
  MONTH      Month of year eg jan, feb, etc
  oneshot    Schedule kron occurrence exactly once
  recurring  Schedule kron occurrence repeatedly

Cisco(config)#kron occurrence saveconfig at 09:30 oneshot ?
  <cr>

Cisco(config)#kron occurrence saveconfig at 09:30 oneshot

Cisco(config-kron-occurrence)#policy-list ?
  WORD  Name of Policy to be executed

Cisco(config-kron-occurrence)#policy-list save-config ?
  <cr>
```

```
Cisco(config-kron-occurrence)#policy-list save-config

Cisco(config-kron-occurrence)#exit

Cisco(config)#exit

Cisco#show kron ?
  schedule  Show when and what occurrences are scheduled

Cisco#show kron schedule ?
  |  Output modifiers
  <cr>

Cisco#show kron schedule
Kron Occurrence Schedule
saveconfig inactive, will run once in 0 days 00:01:19 at 9 :30 on

Cisco#show kron schedule
Kron Occurrence Schedule
(job was completed and since it was a one time run, is now removed from kroon schedule)
```

Chapter 15 Interface or Port Information and Nomenclature

This chapter compares the commands used to collect information about interfaces; configure interface names, speeds, and/or duplex settings; and disable/enable interfaces.

For these commands, it helps if you know how each operating system references ports. ArubaOS-Switch ASIC chassis-based (modular) switches and stackable switches that have a module slot designate ports using the format "slot/port." For example, on the HP 8212 zl switch, port 24 on the module in slot A is referred to as interface A24. Stackable switches simply use the port number.

Comware and Cisco switches (both chassis-based and stackable) designate ports using the format "interface_type slot/sub-slot/port" or "interface_type slot/port."

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch# show interfaces brief	<Comware>display interface brief	Cisco#show interfaces status
ArubaOS-Switch# show interfaces brief 1	<Comware>display interface g1/0/1 brief	Cisco#show interfaces g1/0/1 status
ArubaOS-Switch# show interfaces 1	<Comware>display interface g1/0/1	Cisco#show interfaces g1/0/1
ArubaOS-Switch(config)# interface 1	[Comware]interface g1/0/1	Cisco(config)#interface g1/0/1
ArubaOS-Switch(eth-1)# name link-to-core	[Comware-GigabitEthernet1/0/1]description link-to-core	Cisco(config-if)#description link-to-core
ArubaOS-Switch(eth-1)# speed-duplex auto	[Comware-GigabitEthernet1/0/1]duplex auto	Cisco(config-if)#duplex auto
	[Comware-GigabitEthernet1/0/1]speed auto	Cisco(config-if)#speed auto
ArubaOS-Switch(eth-1)# disable	[Comware-GigabitEthernet1/0/1]shutdown	Cisco(config-if)#shutdown
ArubaOS-Switch(eth-1)# enable	[Comware-GigabitEthernet1/0/1]undo shutdown	Cisco(config-if)#no shutdown
ArubaOS-Switch(config)#allow unsupported-transceiver		Cisco(config)#service unsupported-transceiver
ArubaOS-Switch(config)#allow unsupported-transceiver confirm		

ArubaOS-Switch

```
ArubaOS-Switch# show interfaces ?
 brief                  Show port operational parameters.
 config                 Show port configuration information.
 custom                 Show port parameters in a customized table.
 display                Show summary of network traffic handled by the ports.
 [ethernet] PORT-LIST   Show summary of network traffic handled by the ports.
 port-utilization       Show port bandwidth utilization.
 status                 Show interfaces tagged or untagged VLAN information.
 transceiver            Show the transceiver information.
 tunnel                 Show tunnel configuration and status information.
 <cr>
```

```
ArubaOS-Switch# show interfaces brief ?
 [ethernet] PORT-LIST  Show summary of network traffic handled by the ports.
 <cr>

ArubaOS-Switch# show interfaces brief

Status and Counters - Port Status

                          | Intrusion                                MDI  Flow Bcast
  Port         Type       | Alert     Enabled Status Mode       Mode Ctrl Limit
  ------------ ---------- + --------- ------- ------ ---------- ---- ---- -----
  1            100/1000T  | No        Yes     Up     1000FDx    MDIX off  0
  2            100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  3            100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  4            100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  5            100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  6            100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  7            100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  8            100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  9            100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  10           100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  11           100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  12           100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  13           100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  14           100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  15           100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  16           100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  17           100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  18           100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  19           100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  20           100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  21           100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  22           100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  23           100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  24           100/1000T  | No        Yes     Down   1000FDx    Auto off  0
  25                      | No        Yes     Down   .               off  0
  26                      | No        Yes     Down   .               off  0

ArubaOS-Switch# show interfaces brief 1

 Status and Counters - Port Status

                          | Intrusion                                MDI  Flow Bcast
  Port         Type       | Alert     Enabled Status Mode       Mode Ctrl Limit
  ------------ ---------- + --------- ------- ------ ---------- ---- ---- -----
  1            100/1000T  | No        Yes     Up     1000FDx    MDIX off  0


ArubaOS-Switch# show interfaces 1 ?
 hc                    Show summary of network traffic handled by the ports.
 <cr>

ArubaOS-Switch# show interfaces 1

 Status and Counters - Port Counters for port 1

  Name  :
  MAC Address      : 009c02-d539bf
  Link Status      : Up
  Totals (Since boot or last clear) :
   Bytes Rx        : 2,069,285,321      Bytes Tx        : 214,736,598
   Unicast Rx      : 1,922,572          Unicast Tx      : 1,283,973
   Bcast/Mcast Rx  : 588,985            Bcast/Mcast Tx  : 326,260
```

```
  Errors (Since boot or last clear) :
   FCS Rx          : 0                  Drops Tx        : 0
   Alignment Rx    : 0                  Collisions Tx   : 0
   Runts Rx        : 0                  Late Colln Tx   : 0
   Giants Rx       : 0                  Excessive Colln : 0
   Total Rx Errors : 0                  Deferred Tx     : 0
  Others (Since boot or last clear) :
   Discard Rx      : 0                  Out Queue Len   : 0
   Unknown Protos  : 0
  Rates (5 minute weighted average) :
   Total Rx  (bps) : 510824             Total Tx  (bps) : 517072
   Unicast Rx (Pkts/sec) : 18           Unicast Tx (Pkts/sec) : 20
   B/Mcast Rx (Pkts/sec) : 0            B/Mcast Tx (Pkts/sec) : 0
   Utilization Rx  : 00.51 %            Utilization Tx  : 00.51 %


ArubaOS-Switch(config)# interface ?
 loopback              Enter the loopback Configuration Level.
 [ethernet] PORT-LIST  Enter the Interface Configuration Level, or execute one command
                       for that level.
 tunnel                Enter a tunnel context.

ArubaOS-Switch(config)# interface 1

ArubaOS-Switch(eth-1)#?
 arp-protect           Configure the port as trusted or untrusted.
 bandwidth-min         Enable/disable and configure guaranteed minimum bandwidth
                       settings for outgoing traffic on the port(s).
 broadcast-limit       Limit network bandwidth used by broadcast traffic.
 dhcp-snooping         Configure port-specific DHCP snooping parameters.
 dhcpv6-snooping       Configure DHCPv6 snooping settings on a port.
 disable               Disable interface.
 enable                Enable interface.
 energy-efficient-e... Enables or disables EEE on each port in the port list.
 flow-control          Enable/disable flow control negotiation on the port(s) during
                       link establishment.
 forbid                Prevent ports from becoming a member of specified VLANs.
 gvrp                  Set the GVRP timers for the port.
 ignore-untagged-mac   Prevent MAC address learning for certain untagged control
                       traffic.
 ip                    Apply an access control list to inbound packets on port.
 ipv6                  Configure various IPv6 parameters for the VLAN.
 lacp                  Define whether LACP is enabled on the port, and whether it is in
                       active or passive mode when enabled.
 link-keepalive        Configure UniDirectional Link Detection (UDLD) on the port.
 mac-count-notify      Send a trap when the number of MAC addresses learned on the
                       specified ports exceeds the threshold.
 mac-notify            Configures SNMP traps for changes in the MAC address table.
 mdix-mode             Set port MDI/MDIX mode (default: auto).
 monitor               Monitor traffic on the port.
 name                  Change the interface name.
 poe-allocate-by       Configure the power allocation method.
 poe-lldp-detect       Enabling this feature causes the port to allocate power based on
                       the link-partner's capabilities via LLDP.
 poe-value             Set the maximum power allocation for the port.
 power-over-ethernet   Enable per-port power distribution.
 qos                   Configure port-based traffic prioritization.
 rate-limit            Enable rate limiting for various types of traffic.
 service-policy        Apply the QoS/Mirror policy on the interface.
 smart-link            Configure the control VLANs for receiving flush packets.
 speed-duplex          Define mode of operation for the port(s).
 tagged                Assign ports to specified VLANs as tagged.
 unknown-vlans         Configure the GVRP mode.
```

```
 untagged               Assign ports to specified VLAN as untagged.
 <cr>

ArubaOS-Switch(eth-1)# name ?
 PORT-NAME-STR          Specify a port name up to 64 characters length.

ArubaOS-Switch(eth-1)# name link-to-core


ArubaOS-Switch(eth-1)# speed-duplex ?
 10-half                10 Mbps, half duplex.
 100-half               100 Mbps, half duplex.
 10-full                10 Mbps, full duplex.
 100-full               100 Mbps, full duplex.
 1000-full              1000 Mbps, full duplex.
 auto                   Use Auto Negotiation for speed and duplex mode.
 auto-10                10 Mbps, use Auto Negotiation for duplex mode.
 auto-100               100 Mbps, use Auto Negotiation for duplex mode.
 auto-1000              1000 Mbps, use Auto Negotiation for duplex mode.
 auto-10-100            10 or 100 Mbps, use Auto Negotiation for duplex mode.
 auto-10g               10 Gbps, use Auto Negotiation for duplex mode.

ArubaOS-Switch(eth-1)# speed-duplex auto


ArubaOS-Switch(eth-1)# disable


ArubaOS-Switch(eth-1)# enable
```

Comware5

```
<Comware5>display interface ?
  GigabitEthernet  GigabitEthernet interface
  NULL             NULL interface
  Vlan-interface   VLAN interface
  brief            Brief information of status and configuration for
                   interface(s)
  |                Matching output
  <cr>


<Comware5>display interface brief
The brief information of interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
NULL0                UP   UP(s)    --
Vlan1                UP   UP       10.0.111.31

The brief information of interface(s) under bridge mode:
Link: ADM - administratively down; Stby - standby
Speed or Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
GE1/0/1              UP   1G(a)   F(a)   A    1
GE1/0/2              DOWN auto    A      A    1
GE1/0/3              DOWN auto    A      A    1
GE1/0/4              DOWN auto    A      A    1
GE1/0/5              DOWN auto    A      A    1
GE1/0/6              DOWN auto    A      A    1
GE1/0/7              DOWN auto    A      A    1
GE1/0/8              DOWN auto    A      A    1
GE1/0/9              DOWN auto    A      A    1
```

```
GE1/0/10             DOWN auto    A      A    1
GE1/0/11             DOWN auto    A      A    1
GE1/0/12             DOWN auto    A      A    1
GE1/0/13             DOWN auto    A      A    1
GE1/0/14             DOWN auto    A      A    1
GE1/0/15             DOWN auto    A      A    1
GE1/0/16             DOWN auto    A      A    1
GE1/0/17             DOWN auto    A      A    1
GE1/0/18             DOWN auto    A      A    1
GE1/0/19             DOWN auto    A      A    1
GE1/0/20             DOWN auto    A      A    1
GE1/0/21             DOWN auto    A      A    1
GE1/0/22             DOWN auto    A      A    1
GE1/0/23             DOWN auto    A      A    1
GE1/0/24             DOWN auto    A      A    1
GE1/0/25             ADM  auto    A      A    1
GE1/0/26             ADM  auto    A      A    1
GE1/0/27             ADM  auto    A      A    1
GE1/0/28             ADM  auto    A      A    1


<Comware5>display interface g1/0/1 ?
  brief  Brief information of status and configuration for interface(s)
  |      Matching output
  <cr>

<Comware5>display interface g1/0/1 brief
The brief information of interface(s) under bridge mode:
Link: ADM - administratively down; Stby - standby
Speed or Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
GE1/0/1              UP   1G(a)   F(a)   A    1


<Comware5>display interface g1/0/1
 GigabitEthernet1/0/1 current state: UP
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0023-89d5-a070
 Description: GigabitEthernet1/0/1 Interface
 Loopback is not set
 Media type is twisted pair
 Port hardware type is  1000_BASE_T
 100Mbps-speed mode, full-duplex mode
 Link speed type is autonegotiation, link duplex type is autonegotiation
 Flow-control is not enabled
 The Maximum Frame Length is 9216
 Broadcast MAX-ratio: 100%
 Unicast MAX-ratio: 100%
 Multicast MAX-ratio: 100%
 Allow jumbo frame to pass
 PVID: 1
 Mdi type: auto
 Port link-type: access
  Tagged   VLAN ID : none
  Untagged VLAN ID : 1
 Port priority: 0
 Peak value of input: 213 bytes/sec, at 2015-04-07 00:31:58
 Peak value of output: 236 bytes/sec, at 2015-04-07 00:20:21
 Last 300 seconds input:  2 packets/sec 213 bytes/sec   0%
 Last 300 seconds output:  0 packets/sec 18 bytes/sec   0%
 Input (total):  4311 packets, 1269761 bytes
         781 unicasts, 2272 broadcasts, 1258 multicasts
 Input (normal):  4311 packets, - bytes
```

```
         781 unicasts, 2272 broadcasts, 1258 multicasts
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
 Output (total): 9731 packets, 1114808 bytes
         372 unicasts, 5974 broadcasts, 3385 multicasts, 0 pauses
 Output (normal): 9731 packets, - bytes
         372 unicasts, 5974 broadcasts, 3385 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier


[Comware5]interface ?
  Bridge-Aggregation  Bridge-Aggregation interface
  GigabitEthernet     GigabitEthernet interface
  LoopBack            LoopBack interface
  NULL                NULL interface
  Route-Aggregation   Route-Aggregation interface
  Tunnel              Tunnel interface
  Vlan-interface      VLAN interface
  range               Specify the interface range

[Comware5]interface g1/0/1

[Comware5-GigabitEthernet1/0/1]?
Gigabitethernet_l2 interface view commands:
  apply                  Apply Poe-profile
  arp                    Configure ARP for the interface
  bpdu-drop              Drop BPDU packets.
  bpdu-tunnel            Specify BPDU tunnel function
  broadcast-suppression  Specify the broadcast storm control
  cfd                    Connectivity fault detection (IEEE 802.1ag)
  default                Restore the default settings
  description            Describe the interface
  dhcp-snooping          DHCP Snooping
  display                Display current system information
  dldp                   Specify configuration information of DLDP
  dot1x                  Specify 802.1X configuration information
  duplex                 Status of duplex
  enable                 Enable function
  flow-control           Flow control command
  flow-interval          Set interval of interface statistic
  garp                   Generic Attribute Registration Protocol
  gvrp                   GARP VLAN Registration Protocol
  igmp-snooping          Configure IGMP snooping characteristic
  ip                     Specify IP configurations for the system
  ipv6                   IPv6 status and configuration information
  jumboframe             Jumboframe command
  lacp                   Configure LACP Protocol
  link-aggregation       Link aggregation group
  link-delay             Set the delay time of holding link-up and link-down
  lldp                   Link Layer Discovery Protocol(802.1ab)
  loopback               Specify loopback of current port
  loopback-detection     Detect if loopback exists
  mac-address            Configure MAC address
  mac-authentication     MAC authentication configuration
  mac-forced-forwarding  Specify MAC-forced forwarding configuration
                         information
  mac-vlan               Specify MAC VLAN
  mdi                    Specify mdi type
  mirroring-group        Specify mirroring-group
  mirroring-port         Specify mirroring port
```

```
  mld-snooping            Configure MLD snooping characteristic
  monitor-port            Specify monitor port
  mrp                     Multiple Register Protocol
  mtracert                Trace route to multicast source
  multicast-suppression   Specify the multicast storm control
  mvrp                    Multiple VLAN Registration Protocol
  ndp                     Neighbor discovery protocol
  ntdp                    Specify NTDP configuration information
  oam                     OAM protocol
  packet-filter           Specify packet filter
  ping                    Ping function
  poe                     Configure PoE port
  port                    Configure or modify aggregate parameters on a port
  port-isolate            Specify port-isolate configuration information
  port-security           Specify port-security configuration information
  portal                  Portal protocol
  qinq                    Specify 802.1Q-in-Q VPN function
  qos                     Command of QoS(Quality of Service)
  quit                    Exit from current command view
  return                  Exit to User View
  rmon                    Specify RMON
  save                    Save current configuration
  sflow                   Specify sFlow configuration information
  shutdown                Shut down this interface
  smart-link              Configure smart link
  speed                   Specify speed of current port
  storm-constrain         Port storm-constrain
  stp                     Spanning tree protocol
  tracert                 Trace route function
  undo                    Cancel current setting
  unicast-suppression     Specify the unicast storm control
  virtual-cable-test      Virtual cable test information
  vlan                    Set VLAN precedence
  voice                   Specify voice VLAN

[Comware5-GigabitEthernet1/0/1]description ?
  TEXT  Up to 80 characters for description of the interface

[Comware5-GigabitEthernet1/0/1]description link-to-core


[Comware5-GigabitEthernet1/0/1]duplex ?
  auto  Enable port's duplex negotiation automatically
  full  Full-duplex
  half  Half-duplex

[Comware5-GigabitEthernet1/0/1]duplex auto


[Comware5-GigabitEthernet1/0/1]speed ?
  10    Specify speed as 10 Mbps
  100   Specify speed as 100 Mbps
  1000  Specify speed as 1000 Mbps
  auto  Enable port's speed negotiation automatically

[Comware5-GigabitEthernet1/0/1]speed auto


[Comware5-GigabitEthernet1/0/1]shutdown


[Comware5-GigabitEthernet1/0/1]undo shutdown
```

Comware7

```
<Comware7>display interface ?
  >                     Redirect it to a file
  >>                    Redirect it to a file in append mode
  FortyGigE             FortyGigE interface
  GigabitEthernet       GigabitEthernet interface
  InLoopBack            InLoopBack interface
  M-GigabitEthernet     MGE interface
  NULL                  NULL interface
  Register-Tunnel       Register Tunnel interface
  Ten-GigabitEthernet   Ten-GigabitEthernet interface
  Vlan-interface        VLAN interface
  brief                 Brief information of status and configuration for
                        interface(s)
  range                 Display range information
  |                     Matching output
  <cr>

<Comware7>display interface brief ?
  >            Redirect it to a file
  >>           Redirect it to a file in append mode
  description  Display the complete description information
  down         Display all down ports brief information
  |            Matching output
  <cr>

<Comware7>display interface brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
InLoop0              UP   UP(s)    --
M-GE0/0/0            DOWN DOWN     --
NULL0                UP   UP(s)    --
REG0                 UP   --       --
Vlan1                UP   UP       10.0.111.51

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
FGE1/0/53            DOWN auto    A      A    1
FGE1/0/54            DOWN auto    A      A    1
GE1/0/1              UP   1G(a)   F(a)   A    1
GE1/0/2              DOWN auto    A      A    1
GE1/0/3              DOWN auto    A      A    1
GE1/0/4              DOWN auto    A      A    1
GE1/0/5              DOWN auto    A      A    1
GE1/0/6              DOWN auto    A      A    1
GE1/0/7              DOWN auto    A      A    1
GE1/0/8              DOWN auto    A      A    1
GE1/0/9              DOWN auto    A      A    1
GE1/0/10             DOWN auto    A      A    1
GE1/0/11             DOWN auto    A      A    1
GE1/0/12             DOWN auto    A      A    1
GE1/0/13             DOWN auto    A      A    1
GE1/0/14             DOWN auto    A      A    1
GE1/0/15             DOWN auto    A      A    1
GE1/0/16             DOWN auto    A      A    1
GE1/0/17             DOWN auto    A      A    1
```

```
GE1/0/18              DOWN auto    A      A    1
GE1/0/19              DOWN auto    A      A    1
GE1/0/20              DOWN auto    A      A    1
GE1/0/21              DOWN auto    A      A    1
GE1/0/22              DOWN auto    A      A    1
GE1/0/23              DOWN auto    A      A    1
GE1/0/24              DOWN auto    A      A    1
GE1/0/25              DOWN auto    A      A    1
GE1/0/26              DOWN auto    A      A    1
GE1/0/27              DOWN auto    A      A    1
GE1/0/28              DOWN auto    A      A    1
GE1/0/29              DOWN auto    A      A    1
GE1/0/30              DOWN auto    A      A    1
GE1/0/31              DOWN auto    A      A    1
GE1/0/32              DOWN auto    A      A    1
GE1/0/33              DOWN auto    A      A    1
GE1/0/34              DOWN auto    A      A    1
GE1/0/35              DOWN auto    A      A    1
GE1/0/36              DOWN auto    A      A    1
GE1/0/37              DOWN auto    A      A    1
GE1/0/38              DOWN auto    A      A    1
GE1/0/39              DOWN auto    A      A    1
GE1/0/40              DOWN auto    A      A    1
GE1/0/41              DOWN auto    A      A    1
GE1/0/42              DOWN auto    A      A    1
GE1/0/43              DOWN auto    A      A    1
GE1/0/44              DOWN auto    A      A    1
GE1/0/45              DOWN auto    A      A    1
GE1/0/46              DOWN auto    A      A    1
GE1/0/47              DOWN auto    A      A    1
GE1/0/48              DOWN auto    A      A    1
XGE1/0/49             ADM  auto    A      A    1
XGE1/0/50             ADM  auto    A      A    1
XGE1/0/51             DOWN auto    A      A    1
XGE1/0/52             DOWN auto    A      A    1


<Comware7>display interface g1/0/1 ?
  >      Redirect it to a file
  >>     Redirect it to a file in append mode
  brief  Brief information of status and configuration for interface(s)
  |      Matching output
  <cr>

<Comware7>display interface g1/0/1 brief
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
GE1/0/1              UP   1G(a)   F(a)   A    1


<Comware7>display interface g1/0/1
GigabitEthernet1/0/1
Current state: UP
Line protocol state: UP
IP packet frame type: Ethernet II, hardware address: cc3e-5f73-baf4
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 1000000 kbps
Loopback is not set
Media type is twisted pair
```

```
Port hardware type is 1000_BASE_T
1000Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 10000
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
PVID: 1
MDI type: automdix
Port link-type: Access
 Tagged VLANs:   None
 Untagged VLANs: 1
Port priority: 0
Last clearing of counters: Never
 Peak input rate: 90 bytes/sec, at 2015-04-07 00:31:58
 Peak output rate: 33 bytes/sec, at 2015-04-07 00:22:05
 Last 300 second input: 0 packets/sec 83 bytes/sec 0%
 Last 300 second output: 0 packets/sec 19 bytes/sec 0%
 Input (total):  1728 packets, 215498 bytes
         146 unicasts, 37 broadcasts, 1545 multicasts, 0 pauses
 Input (normal):  1728 packets, - bytes
         146 unicasts, 37 broadcasts, 1545 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
 Output (total): 253 packets, 50800 bytes
         152 unicasts, 10 broadcasts, 91 multicasts, 0 pauses
 Output (normal): 253 packets, - bytes
         152 unicasts, 10 broadcasts, 91 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrierr


[Comware7]interface ?
  Bridge-Aggregation   Bridge-Aggregation interface
  FortyGigE            FortyGigE interface
  GigabitEthernet      GigabitEthernet interface
  LoopBack             LoopBack interface
  M-GigabitEthernet    MGE interface
  NULL                 NULL interface
  Route-Aggregation    Route-Aggregation interface
  Ten-GigabitEthernet  Ten-GigabitEthernet interface
  Tunnel               Tunnel interface
  Vlan-interface       VLAN interface
  range                Configure an interface range

[Comware7]interface g1/0/1

[Comware7-GigabitEthernet1/0/1]?
Gigabitethernet_l2 interface view commands:
  apply                  Apply a PoE profile
  arp                    ARP module
  bandwidth              Specify the expected bandwidth
  bpdu-drop              Specify BPDU drop function
  broadcast-suppression  Broadcast storm suppression function
  cdp                    Non standard IEEE discovery protocol
  cfd                    Connectivity Fault Detection (CFD) module
  dcbx                   Data Center Bridge Capability Exchange Protocol
  default                Restore the default settings
  description            Describe the interface
```

```
  dhcp                    DHCP module
  diagnostic-logfile      Diagnostic log file configuration
  display                 Display current system information
  dldp                    DLDP module
  dot1x                   802.1X module
  duplex                  Status of duplex
  eee                     Energy efficient ethernet
  enable                  Enable functions
  evb                     Edge Virtual Bridging (EVB) module
  flex10                  Configure Flex10
  flow-control            Enable flow control function
  flow-interval           Set the interface statistics interval
  igmp-snooping           IGMP snooping module
  ip                      Specify IP configuration
  ipv6                    Specify IPv6 configuration
  jumboframe              Specify jumbo frame forwarding
  l2vpn                   Layer 2 Virtual Private Network (L2VPN) module
  lacp                    Configure LACP protocol
  link-aggregation        Specify link aggregation group configuration
                          information
  link-delay              Set the physical state change suppression
  lldp                    Link Layer Discovery Protocol(802.1ab)
  logfile                 Log file configuration
  loopback                Specify loopback of current port
  loopback-detection      Loopback detection module
  mac-address             Configure MAC address
  mac-authentication      MAC authentication module
  mac-forced-forwarding   Specify MAC-forced forwarding configuration information
  mac-vlan                MAC VLAN configuration
  mdix-mode               Specify mdix type
  mirroring-group         Specify mirroring group
  mld-snooping            MLD snooping module
  monitor                 System monitor
  mrp                     Multiple registration protocol
  multicast-suppression   Multicast storm suppression function
  mvrp                    Multiple VLAN registration protocol
  oam                     OAM module
  packet-filter           Packet filter settings
  pbb                     Provider Backbone Bridge (PBB) module
  ping                    Ping function
  poe                     Power over Ethernet
  port                    Set port attributes
  port-isolate            Port isolation configuration
  port-security           Port security module
  priority-flow-control   Priority-based flow control (PFC) configuration
  ptp                     Precision Time Protocol (PTP) module
  qcn                     Quantized Congestion Notification (QCN) module
  qinq                    802.1QinQ function
  qos                     Quality of Service (QoS) module
  quit                    Exit from current command view
  return                  Exit to User View
  rmon                    RMON module
  save                    Save current configuration
  security-logfile        Security log file configuration
  service-instance        Configure a service instance
  sflow                   sFlow function
  shutdown                Shut down the interface
  smart-link              Smart Link module
  spbm                    SPBM configuration
  speed                   Specify speed of current port
  storm-constrain         Port storm control
  stp                     Spanning Tree Protocol (STP) module
  tracert                 Tracert function
```

```
  trill                   TRansparent Interconnection of Lots of Links (TRILL)
                          module
  undo                    Cancel current setting
  unicast-suppression     Unicast storm suppression function
  virtual-cable-test      Test cable connection for an interface
  vlan                    Set VLAN precedence
  voice-vlan              Voice VLAN configuration

[Comware7-GigabitEthernet1/0/1]description ?
  TEXT  Interface description, 1 to 255 characters

[Comware-GigabitEthernet1/0/1]description link-to-core


[Comware7-GigabitEthernet1/0/1]duplex ?
  auto  Enable port's duplex negotiation automatically
  full  Full-duplex
  half  Half-duplex

[Comware7-GigabitEthernet1/0/1]duplex auto


[Comware7-GigabitEthernet1/0/1]speed ?
  10    Specify speed as 10 Mbps
  100   Specify speed as 100 Mbps
  1000  Specify speed as 1000 Mbps
  auto  Enable port's speed negotiation automatically

[Comware7-GigabitEthernet1/0/1]speed auto


[Comware7-GigabitEthernet1/0/1]shutdown


[Comware7-GigabitEthernet1/0/1]undo shutdown
```

Cisco

```
Cisco#show interfaces ?
  Async               Async interface
  Auto-Template       Auto-Template interface
  BVI                 Bridge-Group Virtual Interface
  CTunnel             CTunnel interface
  Dialer              Dialer interface
  FastEthernet        FastEthernet IEEE 802.3
  Filter              Filter interface
  Filtergroup         Filter Group interface
  GigabitEthernet     GigabitEthernet IEEE 802.3z
  GroupVI             Group Virtual interface
  Loopback            Loopback interface
  Null                Null interface
  Port-channel        Ethernet Channel of interfaces
  Portgroup           Portgroup interface
  Pos-channel         POS Channel of interfaces
  TenGigabitEthernet  Ten Gigabit Ethernet
  Tunnel              Tunnel interface
  Vif                 PGM Multicast Host interface
  Virtual-Template    Virtual Template interface
  Virtual-TokenRing   Virtual TokenRing
  Vlan                Catalyst Vlans
  accounting          Show interface accounting
  capabilities        Show interface capabilities information
  counters            Show interface counters
  crb                 Show interface routing/bridging info
```

```
  dampening           Show interface dampening info
  debounce            Show interface debounce time info
  description         Show interface description
  etherchannel        Show interface etherchannel information
  fair-queue          Show interface Weighted Fair Queueing (WFQ) info
  fcpa                Fiber Channel
  flowcontrol         Show interface flowcontrol information
  history             Show interface history
  irb                 Show interface routing/bridging info
  mac-accounting      Show interface MAC accounting info
  mpls-exp            Show interface MPLS experimental accounting info
  mtu                 Show interface mtu
  precedence          Show interface precedence accounting info
  private-vlan        Show interface private vlan information
  pruning             Show interface trunk VTP pruning information
  random-detect       Show interface Weighted Random Early Detection (WRED)
                      info
  rate-limit          Show interface rate-limit info
  stats               Show interface packets & octets, in & out, by switching
                      path
  status              Show interface line status
  summary             Show interface summary
  switchport          Show interface switchport information
  transceiver         Show interface transceiver
  trunk               Show interface trunk information
  |                   Output modifiers
  <cr>

Cisco#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/1                      connected    1          a-full a-1000 10/100/1000BaseTX
Gi1/0/2                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/3                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/4                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/5                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/6                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/7                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/8                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/9                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/10                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/11                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/12                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/13                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/14                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/15                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/16                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/17                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/18                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/19                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/20                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/21                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/22                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/23                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/24                     notconnect   1            auto   auto 10/100/1000BaseTX
Te1/0/1                      notconnect   1            full    10G Not Present
Te1/0/2                      notconnect   1            full    10G Not Present
Fa0                          disabled     routed       auto   auto 10/100BaseTX


Cisco#show interfaces g1/0/1 ?
  accounting      Show interface accounting
  capabilities    Show interface capabilities information
```

```
  controller      Show interface status, configuration and controller status
  counters        Show interface counters
  crb             Show interface routing/bridging info
  dampening       Show interface dampening info
  debounce        Show interface debounce time info
  description     Show interface description
  etherchannel    Show interface etherchannel information
  fair-queue      Show interface Weighted Fair Queueing (WFQ) info
  flowcontrol     Show interface flowcontrol information
  history         Show interface history
  irb             Show interface routing/bridging info
  mac-accounting  Show interface MAC accounting info
  mpls-exp        Show interface MPLS experimental accounting info
  mtu             Show interface mtu
  precedence      Show interface precedence accounting info
  private-vlan    Show interface private vlan information
  pruning         Show interface trunk VTP pruning information
  random-detect   Show interface Weighted Random Early Detection (WRED) info
  rate-limit      Show interface rate-limit info
  stats           Show interface packets & octets, in & out, by switching path
  status          Show interface line status
  summary         Show interface summary
  switchport      Show interface switchport information
  transceiver     Show interface transceiver
  trunk           Show interface trunk information
  users           Show interface users
  vlan            Show interface vlan information
  |               Output modifiers
  <cr>

Cisco#show interfaces g1/0/1 status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/1                      connected    1          a-full a-1000 10/100/1000BaseTX


Cisco#show interfaces g1/0/1 status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/1                      connected    1          a-full a-1000 10/100/1000BaseTX

Cisco#show interfaces g1/0/1
GigabitEthernet1/0/1 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 0022.91ab.4381 (bia 0022.91ab.4381)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:07, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1902 packets input, 149768 bytes, 0 no buffer
     Received 1806 broadcasts (1764 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 1764 multicast, 0 pause input
```

```
     0 input packets with dribble condition detected
     482 packets output, 102102 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out


Cisco(config)#interface ?
  Async               Async interface
  Auto-Template       Auto-Template interface
  BVI                 Bridge-Group Virtual Interface
  CTunnel             CTunnel interface
  Dialer              Dialer interface
  FastEthernet        FastEthernet IEEE 802.3
  Filter              Filter interface
  Filtergroup         Filter Group interface
  GigabitEthernet     GigabitEthernet IEEE 802.3z
  Group-Async         Async Group interface
  GroupVI             Group Virtual interface
  Lex                 Lex interface
  Loopback            Loopback interface
  Null                Null interface
  Port-channel        Ethernet Channel of interfaces
  Portgroup           Portgroup interface
  Pos-channel         POS Channel of interfaces
  TenGigabitEthernet  Ten Gigabit Ethernet
  Tunnel              Tunnel interface
  Vif                 PGM Multicast Host interface
  Virtual-Template    Virtual Template interface
  Virtual-TokenRing   Virtual TokenRing
  Vlan                Catalyst Vlans
  fcpa                Fiber Channel
  range               interface range command

Cisco(config)#interface g1/0/1

Cisco(config-if)#?
Interface configuration commands:
  aaa                     Authentication, Authorization and Accounting.
  arp                     Set arp type (arpa, probe, snap) or timeout or log
                          options
  auto                    Configure Automation
  bandwidth               Set bandwidth informational parameter
  bgp-policy              Apply policy propagated by bgp community string
  carrier-delay           Specify delay for interface transitions
  cdp                     CDP interface subcommands
  channel-group           Etherchannel/port bundling configuration
  channel-protocol        Select the channel protocol (LACP, PAgP)
  cts                     Configure Cisco Trusted Security
  dampening               Enable event dampening
  datalink                Interface Datalink commands
  default                 Set a command to its defaults
  delay                   Specify interface throughput delay
  description             Interface specific description
  down-when-looped        Force looped interface down
  duplex                  Configure duplex operation.
  eou                     EAPoUDP Interface Configuration Commands
  exit                    Exit from interface configuration mode
  flow-sampler            Attach flow sampler to the interface
  flowcontrol             Configure flow operation.
  help                    Description of the interactive help system
```

```
  history                  Interface history histograms - 60 second, 60 minute
                           and 72 hour
  hold-queue               Set hold queue depth
  ip                       Interface Internet Protocol config commands
  keepalive                Enable keepalive
  l2protocol-tunnel        Tunnel Layer2 protocols
  lacp                     LACP interface subcommands
  link                     Configure Link
  lldp                     LLDP interface subcommands
  load-interval            Specify interval for load calculation for an
                           interface
  location                 Interface location information
  logging                  Configure logging for interface
  mac                      MAC interface commands
  macro                    Command macro
  max-reserved-bandwidth   Maximum Reservable Bandwidth on an Interface
  mdix                     Set Media Dependent Interface with Crossover
  mka                      MACsec Key Agreement (MKA) interface configuration
  mls                      mls interface commands
  mvr                      MVR per port configuration
  neighbor                 interface neighbor configuration mode commands
  network-policy           Network Policy
  nmsp                     NMSP interface configuration
  no                       Negate a command or set its defaults
  pagp                     PAgP interface subcommands
  priority-queue           Priority Queue
  queue-set                Choose a queue set for this queue
  rmon                     Configure Remote Monitoring on an interface
  routing                  Per-interface routing configuration
  rsu                      rollsing stack upgrade
  service-policy           Configure CPL Service Policy
  shutdown                 Shutdown the selected interface
  small-frame              Set rate limit parameters for small frame
  snmp                     Modify SNMP interface parameters
  source                   Get config from another source
  spanning-tree            Spanning Tree Subsystem
  speed                    Configure speed operation.
  srr-queue                Configure shaped round-robin transmit queues
  storm-control            storm configuration
  switchport               Set switching mode characteristics
  timeout                  Define timeout values for this interface
  topology                 Configure routing topology on the interface
  transmit-interface       Assign a transmit interface to a receive-only
                           interface
  tx-ring-limit            Configure PA level transmit ring limit
  udld                     Configure UDLD enabled or disabled and ignore global
                           UDLD setting
  vtp                      Enable VTP on this interface


Cisco(config-if)#description ?
  LINE  Up to 200 characters describing this interface

Cisco(config-if)#description link-to-core


Cisco(config-if)#duplex ?
  auto  Enable AUTO duplex configuration
  full  Force full duplex operation
  half  Force half-duplex operation

Cisco(config-if)#duplex auto
```

```
Cisco(config-if)#speed ?
  10    Force 10 Mbps operation
  100   Force 100 Mbps operation
  1000  Force 1000 Mbps operation
  auto  Enable AUTO speed configuration

Cisco(config-if)#speed auto


Cisco(config-if)#shutdown


Cisco(config-if)#no shutdown
```

Chapter 16 VLAN Management

This chapter compares the commands that are used to configure VLANs.

In Cisco and Comware, for example, the term *trunk* refers to an interface that you configure to support 802.1Q VLAN tagged frames. That is, an interface that you configure to support multiple VLANs is a *trunk* interface in each VLAN in Cisco and Comware. In the ArubaOS-Switch operating system, on the other hand, an interface that supports multiple VLANs is a *tagged* interface in each VLAN.

In addition, ArubaOS-Switch referes to aggregated interfaces as a *trunk*. In Comware the term is *bridge aggregation*, while on Cisco it is *EtherChannel*.

Interface use	ArubaOS-Switch	Comware	Cisco
Non-802.1Q interfaces (such as used for computers or printers)	untagged	access	access
802.1Q interfaces (such as used for switch-to-switch, switch-to-server, and switch-to-VoIP phones)	tagged	trunk (Note: some display views will denote tagged)	trunk
Aggregated interfaces	trunk	bridge aggregation	etherchannel

a) Creating and Naming VLANs

ArubaOS-Switch	Comware	Cisco
`ArubaOS-Switch(config)# vlan 220`	`[Comware]vlan 220`	`Cisco(config)#vlan 220`
`ArubaOS-Switch(vlan-220)# name test`	`[Comware-vlan220]name test`	`Cisco(config-vlan)#name test`
`ArubaOS-Switch# show vlans`	`[Comware]display vlan`	`Cisco#show vlan brief`
	`[Comware]display vlan all`	

ArubaOS-Switch

```
ArubaOS-Switch(config)# vlan 220

ArubaOS-Switch(vlan-220)# ?
 connection-rate-fi... Re-enables access to a host or set of hosts previously blocked by
                       the connection rate filter.
 dhcp-server           Enable the DHCP service on the VLAN.
 dhcp-snooping         Enable DHCP snooping on the VLAN.
 dhcpv6-snooping       Enable DHCPv6 snooping on the VLAN.
 disable               Enable or disable various features on the device.
 forbid                Prevent ports from becoming a member of the current VLAN.
 igmp-proxy            Associate an IGMP proxy domain with a VLAN.
 ip                    Configure various IP parameters for the VLAN.
 ip-recv-mac-address   Associates a L3-mac-address with a VLAN.
 ipv6                  Configure various IPv6 parameters for the VLAN.
 jumbo                 Labels this VLAN as a Jumbo VLAN, allowing you to pass packets up
                       to 9216 bytes in size.
 monitor               Define either the VLAN is to be monitored or not.
 name                  Set the VLAN's name.
 portal                Enable BYOD redirection on this VLAN.
 protocol              Set a predefined protocol for the current VLAN.
 qos                   Configure VLAN-based traffic prioritization.
```

```
 service-policy        Apply the QoS/Mirror policy on the vlan.
 tagged                Assign ports to current VLAN as tagged.
 untagged              Assign ports to current VLAN as untagged.
 voice                 Usage: [no] voiceDescription: Labels this VLAN as a Voice VLAN,
                       allowing you to separate, prioritize, and authenticate voice
                       traffic moving through your network.
 vrrp                  Enable/configure VRRP operation on the VLAN.

ArubaOS-Switch(vlan-220)# name ?
 ASCII-STR             Enter an ASCII string.

ArubaOS-Switch(vlan-220)# name test
```

(also as compound statement)

```
ArubaOS-Switch(config)# vlan 230 name test2


ArubaOS-Switch(config)# show vlans ?
 custom                Show vlan parameters in customized order.
 ports                 Show VLANs that have at least one port from the 'PORT-LIST' as a
                       member.
 VLAN-ID               Show detailed VLAN information for the VLAN with the ID supplied.
 <cr>

ArubaOS-Switch(config)# show vlans

 Status and Counters - VLAN Information

  Maximum VLANs to support : 256
  Primary VLAN : DEFAULT_VLAN
  Management VLAN :

  VLAN ID Name                             | Status     Voice Jumbo
  ------- -------------------------------- + ---------- ----- -----
  1       DEFAULT_VLAN                     | Port-based No    No
  100     VLAN100                          | Port-based No    No
  220     test                             | Port-based No    No
  230     test2                            | Port-based No    No
```

Comware5

```
[Comware5]vlan 220

[Comware5-vlan220]?
Vlan view commands:
  arp                     Specify ARP configuration information
  arp-snooping            ARP snooping
  cfd                     Connectivity fault detection (IEEE 802.1ag)
  description             Description of VLAN
  display                 Display current system information
  igmp-snooping           IGMP snooping
  ip-subnet-vlan          IP subnet-based VLAN
  ipv6                    IPv6 status and configuration information
  isolate-user-vlan       Specify isolate-user-VLAN characteristic
  isolated-vlan           Specify isolated VLAN characteristic
  mac-address             Configure MAC address
  mac-forced-forwarding   Specify MAC-forced forwarding configuration
                          information
  mld-snooping            Configure MLD snooping characteristic
  mtracert                Trace route to multicast source
  name                    Name of VLAN
  pim-snooping            Configure PIM snooping characteristic
```

```
  ping                    Ping function
  port                    Add ports to or delete ports from VLAN
  protocol-vlan           Protocol-based VLAN
  quit                    Exit from current command view
  return                  Exit to User View
  save                    Save current configuration
  subvlan                 Specify Sub VLAN
  supervlan               Specify the VLAN to be a Super VLAN
  tracert                 Trace route function
  undo                    Cancel current setting

[Comware5-vlan220]name ?
  TEXT  Up to 32 characters for name of this VLAN

[Comware5-vlan220]name test


[Comware5]display vlan ?
  INTEGER<1-4094>  VLAN ID
  all              All the VLANs
  dynamic          Dynamic VLAN ID
  reserved         Reserved VLAN ID
  static           Static VLAN ID
  |                Matching output
  <cr>

[Comware5]display vlan
 Total 3 VLAN exist(s).
 The following VLANs exist:
  1(default), 100, 220,

[Comware5]display vlan all
 VLAN ID: 1
 VLAN Type: static
 Route Interface: configured
 IPv4 address: 10.0.111.31
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged   Ports: none
 Untagged Ports:
    GigabitEthernet1/0/1     GigabitEthernet1/0/2     GigabitEthernet1/0/3
    GigabitEthernet1/0/4     GigabitEthernet1/0/5     GigabitEthernet1/0/6
    GigabitEthernet1/0/7     GigabitEthernet1/0/8     GigabitEthernet1/0/9
    GigabitEthernet1/0/10    GigabitEthernet1/0/11    GigabitEthernet1/0/12
    GigabitEthernet1/0/13    GigabitEthernet1/0/14    GigabitEthernet1/0/15
    GigabitEthernet1/0/16    GigabitEthernet1/0/17    GigabitEthernet1/0/18
    GigabitEthernet1/0/19    GigabitEthernet1/0/20    GigabitEthernet1/0/21
    GigabitEthernet1/0/22    GigabitEthernet1/0/23    GigabitEthernet1/0/24
    GigabitEthernet1/0/25    GigabitEthernet1/0/26    GigabitEthernet1/0/27
    GigabitEthernet1/0/28

 VLAN ID: 100
 VLAN Type: static
 Route Interface: not configured
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged   Ports: none
 Untagged Ports: none

 VLAN ID: 220
 VLAN Type: static
 Route Interface: not configured
```

```
 Description: VLAN 0220
 Name: test
 Tagged   Ports: none
 Untagged Ports: none
```

Comware7

```
[Comware7]vlan 220

[Comware7-vlan220]?
Vlan view commands:
  arp                     ARP module
  cfd                     Connectivity Fault Detection (CFD) module
  description             Configure the VLAN description
  diagnostic-logfile      Diagnostic log file configuration
  display                 Display current system information
  igmp-snooping           IGMP snooping module
  ip-subnet-vlan
  ipv6                    Specify IPv6 configuration
  logfile                 Log file configuration
  mac-address             Configure MAC address
  mac-forced-forwarding   Specify MAC-forced forwarding configuration information
  mld-snooping            MLD snooping module
  monitor                 System monitor
  name                    Configure the VLAN name
  pim-snooping            PIM snooping module
  ping                    Ping function
  port                    Assign ports to or remove ports from the VLAN
  private-vlan            Private VLAN function
  protocol-vlan           Protocol-based VLAN
  quit                    Exit from current command view
  return                  Exit to User View
  save                    Save current configuration
  security-logfile        Security log file configuration
  subvlan                 Specify sub-VLAN
  supervlan               Specify the VLAN as a super VLAN
  tracert                 Tracert function
  undo                    Cancel current setting

[Comware7-vlan220]name ?
  TEXT  Name string, 32 characters at most

[Comware7-vlan220]name test


[Comware7]display vlan ?
  >                Redirect it to a file
  >>               Redirect it to a file in append mode
  INTEGER<1-4094>  VLAN ID
  all              All VLANs
  brief            Brief information about all VLANs
  dynamic          Dynamic VLANs
  mapping          Display VLAN mapping information
  reserved         Reserved VLANs
  static           Static VLANs
  |                Matching output
  <cr>

[Comware7]display vlan
 Total VLANs: 3
 The VLANs include:
 1(default), 100, 220

[Comware7]display vlan all
```

```
 VLAN ID: 1
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 10.0.111.51
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports:
    FortyGigE1/0/53               FortyGigE1/0/54
    GigabitEthernet1/0/1          GigabitEthernet1/0/2
    GigabitEthernet1/0/3          GigabitEthernet1/0/4
    GigabitEthernet1/0/5          GigabitEthernet1/0/6
    GigabitEthernet1/0/7          GigabitEthernet1/0/8
    GigabitEthernet1/0/9          GigabitEthernet1/0/10
    GigabitEthernet1/0/11         GigabitEthernet1/0/12
    GigabitEthernet1/0/13         GigabitEthernet1/0/14
    GigabitEthernet1/0/15         GigabitEthernet1/0/16
    GigabitEthernet1/0/17         GigabitEthernet1/0/18
    GigabitEthernet1/0/19         GigabitEthernet1/0/20
    GigabitEthernet1/0/21         GigabitEthernet1/0/22
    GigabitEthernet1/0/23         GigabitEthernet1/0/24
    GigabitEthernet1/0/25         GigabitEthernet1/0/26
    GigabitEthernet1/0/27         GigabitEthernet1/0/28
    GigabitEthernet1/0/29         GigabitEthernet1/0/30
    GigabitEthernet1/0/31         GigabitEthernet1/0/32
    GigabitEthernet1/0/33         GigabitEthernet1/0/34
    GigabitEthernet1/0/35         GigabitEthernet1/0/36
    GigabitEthernet1/0/37         GigabitEthernet1/0/38
    GigabitEthernet1/0/39         GigabitEthernet1/0/40
    GigabitEthernet1/0/41         GigabitEthernet1/0/42
    GigabitEthernet1/0/43         GigabitEthernet1/0/44
    GigabitEthernet1/0/45         GigabitEthernet1/0/46
    GigabitEthernet1/0/47         GigabitEthernet1/0/48
    Ten-GigabitEthernet1/0/49
    Ten-GigabitEthernet1/0/50
    Ten-GigabitEthernet1/0/51
    Ten-GigabitEthernet1/0/52

 VLAN ID: 100
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged ports:   None
 Untagged ports: None

 VLAN ID: 220
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0220
 Name: test
 Tagged ports:   None
 Untagged ports: None
```

Cisco

```
Cisco(config)#vlan 220

Cisco(config-vlan)#?
VLAN configuration commands:
  are           Maximum number of All Route Explorer hops for this VLAN (or
                zero if none specified)
  backupcrf     Backup CRF mode of the VLAN
```

```
  bridge        Bridging characteristics of the VLAN
  exit          Apply changes, bump revision number, and exit mode
  media         Media type of the VLAN
  mtu           VLAN Maximum Transmission Unit
  name          Ascii name of the VLAN
  no            Negate a command or set its defaults
  parent        ID number of the Parent VLAN of FDDI or Token Ring type VLANs
  private-vlan  Configure a private VLAN
  remote-span   Configure as Remote SPAN VLAN
  ring          Ring number of FDDI or Token Ring type VLANs
  said          IEEE 802.10 SAID
  shutdown      Shutdown VLAN switching
  state         Operational state of the VLAN
  ste           Maximum number of Spanning Tree Explorer hops for this VLAN (or
                zero if none specified)
  stp           Spanning tree characteristics of the VLAN
  tb-vlan1      ID number of the first translational VLAN for this VLAN (or
                zero if none)
  tb-vlan2      ID number of the second translational VLAN for this VLAN (or
                zero if none)

Cisco(config-vlan)#name ?
  WORD  The ascii name for the VLAN

Cisco(config-vlan)#name test


Cisco#show vlan ?
  access-log    VACL Logging
  access-map    Vlan access-map
  brief         VTP all VLAN status in brief
  dot1q         Display dot1q parameters
  filter        VLAN filter information
  group         VLAN group(s) information
  id            VTP VLAN status by VLAN id
  ifindex       SNMP ifIndex
  internal      VLAN internal usage
  mtu           VLAN MTU information
  name          VTP VLAN status by VLAN name
  private-vlan  Private VLAN information
  remote-span   Remote SPAN VLANs
  summary       VLAN summary information
  |             Output modifiers
  <cr>

Cisco#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                                                Gi1/0/4, Gi1/0/5, Gi1/0/6
                                                Gi1/0/7, Gi1/0/8, Gi1/0/9
                                                Gi1/0/10, Gi1/0/11, Gi1/0/12
                                                Gi1/0/13, Gi1/0/14, Gi1/0/15
                                                Gi1/0/16, Gi1/0/17, Gi1/0/18
                                                Gi1/0/19, Gi1/0/20, Gi1/0/21
                                                Gi1/0/22, Gi1/0/23, Gi1/0/24
                                                Te1/0/1, Te1/0/2
100  VLAN0100                         active
220  test                             active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
```

```
1005 trnet-default                      act/unsup
```

b) Assigning Ports or Interfaces to VLANs

ArubaOS-Switch	Comware	Cisco
(tag/untag)	(trunk/access)	(trunk/access)
ArubaOS-Switch(config)# vlan 220	[Comware]interface g1/0/6	Cisco(config)#interface g1/0/6
ArubaOS-Switch(vlan-220)# tagged 6	[Comware-GigabitEthernet1/0/6]port link-type trunk [Comware-GigabitEthernet1/0/6]port trunk permit vlan 220	Cisco(config-if)#switchport trunk encapsulation dot1q Cisco(config-if)#switchport trunk allowed vlan 220 Cisco(config-if)#switchport mode trunk Cisco(config-if)#switchport nonegotiate
ArubaOS-Switch(vlan-220)# untagged 4	[Comware]vlan 220 [Comware-vlan220]port g1/0/4	Cisco(config)#interface g1/0/4 Cisco(config-if)#switchport Cisco(config-if)#switchport access vlan 220 Cisco(config-if)#switchport mode access
ArubaOS-Switch# show vlans 220 ArubaOS-Switch# show vlans 100 ArubaOS-Switch# show vlans 1	[Comware]display vlan 220 [Comware]display vlan 100 [Comware]display vlan 1	Cisco#show vlan id 220 Cisco#show vlan id 100 Cisco#show vlan id 1
ArubaOS-Switch# show vlans ports 6 detail	[Comware]display interface g1/0/6	Cisco#show interfaces g1/0/6 switchport
ArubaOS-Switch# show vlans ports 5 detail	[Comware]display interface g1/0/5	Cisco#show interfaces g1/0/5 switchport

ArubaOS-Switch

```
ArubaOS-Switch(config)# vlan 220

ArubaOS-Switch(vlan-220)# tagged 6
```

(also as compound statement)

```
ArubaOS-Switch(config)# vlan 220 tagged 6


ArubaOS-Switch(config)# vlan 220

ArubaOS-Switch(vlan-220)# untagged 5
```

(also as compound statement)

```
ArubaOS-Switch(config)# vlan 220 untagged 5
```

```
ArubaOS-Switch# show vlans 220

 Status and Counters - VLAN Information - VLAN 220

  VLAN ID : 220
  Name : test
  Status : Port-based
  Voice : No
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  4                Untagged Learn        Down
  6                Tagged   Learn        Down


ArubaOS-Switch# show vlans 100

 Status and Counters - VLAN Information - VLAN 100

  VLAN ID : 100
  Name : VLAN100
  Status : Port-based
  Voice : No
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  5                Untagged Learn        Down
  6                Tagged   Learn        Down
  9                Untagged Learn        Down


ArubaOS-Switch# show vlans 1

 Status and Counters - VLAN Information - VLAN 1

  VLAN ID : 1
  Name : DEFAULT_VLAN
  Status : Port-based
  Voice : No
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  1                Untagged Learn        Up
  2                Untagged Learn        Down
  3                Untagged Learn        Down
  6                Untagged Learn        Down
  7                Untagged Learn        Down
  8                Untagged Learn        Down
  10               Untagged Learn        Down
  11               Untagged Learn        Up
  12               Untagged Learn        Down
  13               Untagged Learn        Up
  14               Untagged Learn        Down
  15               Untagged Learn        Down
  16               Untagged Learn        Down
  17               Untagged Learn        Down
  18               Untagged Learn        Down
  19               Untagged Learn        Down
  20               Untagged Learn        Down
```

```
  21                Untagged Learn        Down
  22                Untagged Learn        Down
  23                Untagged Learn        Down
  24                Untagged Learn        Down
  25                Untagged Learn        Down
  26                Untagged Learn        Down

  Overridden Port VLAN configuration

  Port   Mode
  ------ ------------

ArubaOS-Switch# show vlans ports 6 detail

 Status and Counters - VLAN Information - for ports 6

  VLAN ID Name                 | Status     Voice Jumbo Mode
  ------- -------------------- + ---------- ----- ----- --------
  1       DEFAULT_VLAN         | Port-based No    No    Untagged
  100     VLAN100              | Port-based No    No    Tagged
  220     test                 | Port-based No    No    Tagged


ArubaOS-Switch# show vlans ports 5 detail

 Status and Counters - VLAN Information - for ports 5

  VLAN ID Name                 | Status     Voice Jumbo Mode
  ------- -------------------- + ---------- ----- ----- --------
  100     VLAN100              | Port-based No    No    Untagged
```

Comware5

```
[Comware5]interface g1/0/6

[Comware5-GigabitEthernet1/0/6]port link-type ?
  access  Access link-type
  hybrid  Hybrid VLAN link-type
  trunk   VLAN Trunk link-type

[Comware5-GigabitEthernet1/0/6]?
Gigabitethernet_l2 interface view commands:
  apply                  Apply Poe-profile
  arp                    Configure ARP for the interface
  bpdu-drop              Drop BPDU packets.
  bpdu-tunnel            Specify BPDU tunnel function
  broadcast-suppression  Specify the broadcast storm control
  cfd                    Connectivity fault detection (IEEE 802.1ag)
  default                Restore the default settings
  description            Describe the interface
  dhcp-snooping          DHCP Snooping
  display                Display current system information
  dldp                   Specify configuration information of DLDP
  dot1x                  Specify 802.1X configuration information
  duplex                 Status of duplex
  enable                 Enable function
  flow-control           Flow control command
  flow-interval          Set interval of interface statistic
  garp                   Generic Attribute Registration Protocol
  gvrp                   GARP VLAN Registration Protocol
  igmp-snooping          Configure IGMP snooping characteristic
  ip                     Specify IP configurations for the system
  ipv6                   IPv6 status and configuration information
  jumboframe             Jumboframe command
```

```
  lacp                    Configure LACP Protocol
  link-aggregation        Link aggregation group
  link-delay              Set the delay time of holding link-up and link-down
  lldp                    Link Layer Discovery Protocol(802.1ab)
  loopback                Specify loopback of current port
  loopback-detection      Detect if loopback exists
  mac-address             Configure MAC address
  mac-authentication      MAC authentication configuration
  mac-forced-forwarding   Specify MAC-forced forwarding configuration
                          information
  mac-vlan                Specify MAC VLAN
  mdi                     Specify mdi type
  mirroring-group         Specify mirroring-group
  mirroring-port          Specify mirroring port
  mld-snooping            Configure MLD snooping characteristic
  monitor-port            Specify monitor port
  mrp                     Multiple Register Protocol
  mtracert                Trace route to multicast source
  multicast-suppression   Specify the multicast storm control
  mvrp                    Multiple VLAN Registration Protocol
  ndp                     Neighbor discovery protocol
  ntdp                    Specify NTDP configuration information
  oam                     OAM protocol
  packet-filter           Specify packet filter
  ping                    Ping function
  poe                     Configure PoE port
  port                    Configure or modify aggregate parameters on a port
  port-isolate            Specify port-isolate configuration information
  port-security           Specify port-security configuration information
  portal                  Portal protocol
  qinq                    Specify 802.1Q-in-Q VPN function
  qos                     Command of QoS(Quality of Service)
  quit                    Exit from current command view
  return                  Exit to User View
  rmon                    Specify RMON
  save                    Save current configuration
  sflow                   Specify sFlow configuration information
  shutdown                Shut down this interface
  smart-link              Configure smart link
  speed                   Specify speed of current port
  storm-constrain         Port storm-constrain
  stp                     Spanning tree protocol
  tracert                 Trace route function
  undo                    Cancel current setting
  unicast-suppression     Specify the unicast storm control
  virtual-cable-test      Virtual cable test information
  vlan                    Set VLAN precedence
  voice                   Specify voice VLAN

[Comware5-GigabitEthernet1/0/6]port ?
  access              Specify current Access port's characteristics
  auto-power-down     Auto power down mode
  bridge              Configure port bridge
  hybrid              Specify current Hybrid port's characteristics
  isolate-user-vlan   Specify isolate-user-VLAN characteristic
  link-aggregation    Link aggregation group
  link-mode           Switch the specified interface to layer2 or layer3
                      ethernet
  link-type           Specify port link-type
  monitor-link        Specify monitor link
  multicast-vlan      Multicast VLAN
  pvid                Set port PVID
  service-loopback    Service loop back group
```

```
  smart-link         Specify smart link
  trunk              Specify current Trunk port's characteristics

[Comware5-GigabitEthernet1/0/6]port link-type ?
  access  Access link-type
  hybrid  Hybrid VLAN link-type
  trunk   VLAN Trunk link-type

[Comware5-GigabitEthernet1/0/6]port link-type trunk


[Comware5-GigabitEthernet1/0/6]port trunk ?
  permit  Allowed VLANs
  pvid    Specify current Trunk port's PVID VLAN characteristics

[Comware5-GigabitEthernet1/0/6]port trunk permit ?
  vlan  Allowed VLAN

[Comware5-GigabitEthernet1/0/6]port trunk permit vlan ?
  INTEGER<1-4094>  VLAN ID
  all              All the VLANs

[Comware5-GigabitEthernet1/0/6]port trunk permit vlan 100 220


[Comware5]vlan 220

[Comware5-vlan220]?
Vlan view commands:
  arp                     Specify ARP configuration information
  arp-snooping            ARP snooping
  cfd                     Connectivity fault detection (IEEE 802.1ag)
  description             Description of VLAN
  display                 Display current system information
  igmp-snooping           IGMP snooping
  ip-subnet-vlan          IP subnet-based VLAN
  ipv6                    IPv6 status and configuration information
  isolate-user-vlan       Specify isolate-user-VLAN characteristic
  isolated-vlan           Specify isolated VLAN characteristic
  mac-address             Configure MAC address
  mac-forced-forwarding   Specify MAC-forced forwarding configuration
                          information
  mld-snooping            Configure MLD snooping characteristic
  mtracert                Trace route to multicast source
  name                    Name of VLAN
  pim-snooping            Configure PIM snooping characteristic
  ping                    Ping function
  port                    Add ports to or delete ports from VLAN
  protocol-vlan           Protocol-based VLAN
  quit                    Exit from current command view
  return                  Exit to User View
  save                    Save current configuration
  subvlan                 Specify Sub VLAN
  supervlan               Specify the VLAN to be a Super VLAN
  tracert                 Trace route function
  undo                    Cancel current setting

[Comware5-vlan220]port ?
  GigabitEthernet  GigabitEthernet interface

[Comware5-vlan220]port g1/0/4 ?
  GigabitEthernet  GigabitEthernet interface
  to               Range of interfaces
```

```
  <cr>

[Comware5-vlan220]port g1/0/4


[Comware5]display vlan 220
 VLAN ID: 220
 VLAN Type: static
 Route Interface: not configured
 Description: VLAN 0220
 Name: test
 Tagged   Ports:
    GigabitEthernet1/0/6
 Untagged Ports:
    GigabitEthernet1/0/4

[Comware5]display vlan 100
 VLAN ID: 100
 VLAN Type: static
 Route Interface: not configured
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged   Ports:
    GigabitEthernet1/0/6
 Untagged Ports:
    GigabitEthernet1/0/5     GigabitEthernet1/0/9

[Comware5]display vlan 1
 VLAN ID: 1
 VLAN Type: static
 Route Interface: configured
 IPv4 address: 10.0.111.31
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged   Ports: none
 Untagged Ports:
    GigabitEthernet1/0/1     GigabitEthernet1/0/2     GigabitEthernet1/0/3
    GigabitEthernet1/0/6     GigabitEthernet1/0/7     GigabitEthernet1/0/8
    GigabitEthernet1/0/10    GigabitEthernet1/0/11    GigabitEthernet1/0/12
    GigabitEthernet1/0/13    GigabitEthernet1/0/14    GigabitEthernet1/0/15
    GigabitEthernet1/0/16    GigabitEthernet1/0/17    GigabitEthernet1/0/18
    GigabitEthernet1/0/19    GigabitEthernet1/0/20    GigabitEthernet1/0/21
    GigabitEthernet1/0/22    GigabitEthernet1/0/23    GigabitEthernet1/0/24
    GigabitEthernet1/0/25    GigabitEthernet1/0/26    GigabitEthernet1/0/27
    GigabitEthernet1/0/28


[Comware5]display interface g1/0/6
 GigabitEthernet1/0/6 current state: UP
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0023-89d5-a075
 Description: GigabitEthernet1/0/6 Interface
 Loopback is not set
 Media type is twisted pair
 Port hardware type is  1000_BASE_T
 1000Mbps-speed mode, full-duplex mode
 Link speed type is autonegotiation, link duplex type is autonegotiation
 Flow-control is not enabled
 The Maximum Frame Length is 9216
 Broadcast MAX-ratio: 100%
 Unicast MAX-ratio: 100%
 Multicast MAX-ratio: 100%
 Allow jumbo frame to pass
```

```
 PVID: 1
 Mdi type: auto
 Port link-type: trunk
  VLAN passing  : 1(default vlan), 100, 220
  VLAN permitted: 1(default vlan), 100, 220
  Trunk port encapsulation: IEEE 802.1q
 Port priority: 0
 Last clearing of counters:  Never
 Peak value of input: 16 bytes/sec, at 2015-04-08 02:29:34
 Peak value of output: 9 bytes/sec, at 2015-04-08 02:29:34
 Last 300 seconds input:  0 packets/sec 21 bytes/sec 0%
 Last 300 seconds output:  0 packets/sec 9 bytes/sec 0%
 Input (total):  56 packets, 6492 bytes
         0 unicasts, 16 broadcasts, 40 multicasts, 0 pauses
 Input (normal):  56 packets, - bytes
         0 unicasts, 16 broadcasts, 40 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
 Output (total): 14 packets, 2732 bytes
         5 unicasts, 0 broadcasts, 9 multicasts, 0 pauses
 Output (normal): 14 packets, - bytes
         5 unicasts, 0 broadcasts, 9 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier


[Comware5]display interface g1/0/5
 GigabitEthernet1/0/5 current state: DOWN
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0023-89d5-a074
 Description: GigabitEthernet1/0/5 Interface
 Loopback is not set
 Media type is twisted pair
 Port hardware type is  1000_BASE_T
 Unknown-speed mode, unknown-duplex mode
 Link speed type is autonegotiation, link duplex type is autonegotiation
 Flow-control is not enabled
 The Maximum Frame Length is 9216
 Broadcast MAX-ratio: 100%
 Unicast MAX-ratio: 100%
 Multicast MAX-ratio: 100%
 Allow jumbo frame to pass
 PVID: 100
 Mdi type: auto
 Port link-type: access
  Tagged   VLAN ID : none
  Untagged VLAN ID : 100
 Port priority: 0
 Last clearing of counters:  Never
 Peak value of input: 0 bytes/sec, at 2000-04-26 06:02:01
 Peak value of output: 0 bytes/sec, at 2000-04-26 06:02:01
 Last 300 seconds input:  0 packets/sec 0 bytes/sec -%
 Last 300 seconds output:  0 packets/sec 0 bytes/sec -%
 Input (total):  0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input (normal):  0 packets, - bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
 Output (total): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
```

```
 Output (normal): 0 packets, - bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier
```

Comware7

```
[Comware7]interface g1/0/6

[Comware7-GigabitEthernet1/0/6]?
Gigabitethernet_l2 interface view commands:
  apply                   Apply a PoE profile
  arp                     ARP module
  bandwidth               Specify the expected bandwidth
  bpdu-drop               Specify BPDU drop function
  broadcast-suppression   Broadcast storm suppression function
  cdp                     Non standard IEEE discovery protocol
  cfd                     Connectivity Fault Detection (CFD) module
  dcbx                    Data Center Bridge Capability Exchange Protocol
  default                 Restore the default settings
  description             Describe the interface
  dhcp                    DHCP module
  diagnostic-logfile      Diagnostic log file configuration
  display                 Display current system information
  dldp                    DLDP module
  dot1x                   802.1X module
  duplex                  Status of duplex
  eee                     Energy efficient ethernet
  enable                  Enable functions
  evb                     Edge Virtual Bridging (EVB) module
  flex10                  Configure Flex10
  flow-control            Enable flow control function
  flow-interval           Set the interface statistics interval
  igmp-snooping           IGMP snooping module
  ip                      Specify IP configuration
  ipv6                    Specify IPv6 configuration
  jumboframe              Specify jumbo frame forwarding
  l2vpn                   Layer 2 Virtual Private Network (L2VPN) module
  lacp                    Configure LACP protocol
  link-aggregation        Specify link aggregation group configuration
                          information
  link-delay              Set the physical state change suppression
  lldp                    Link Layer Discovery Protocol(802.1ab)
  logfile                 Log file configuration
  loopback                Specify loopback of current port
  loopback-detection      Loopback detection module
  mac-address             Configure MAC address
  mac-authentication      MAC authentication module
  mac-forced-forwarding   Specify MAC-forced forwarding configuration information
  mac-vlan                MAC VLAN configuration
  mdix-mode               Specify mdix type
  mirroring-group         Specify mirroring group
  mld-snooping            MLD snooping module
  monitor                 System monitor
  mrp                     Multiple registration protocol
  multicast-suppression   Multicast storm suppression function
  mvrp                    Multiple VLAN registration protocol
  oam                     OAM module
  packet-filter           Packet filter settings
  pbb                     Provider Backbone Bridge (PBB) module
  ping                    Ping function
  poe                     Power over Ethernet
  port                    Set port attributes
```

```
  port-isolate           Port isolation configuration
  port-security          Port security module
  priority-flow-control  Priority-based flow control (PFC) configuration
  ptp                    Precision Time Protocol (PTP) module
  qcn                    Quantized Congestion Notification (QCN) module
  qinq                   802.1QinQ function
  qos                    Quality of Service (QoS) module
  quit                   Exit from current command view
  return                 Exit to User View
  rmon                   RMON module
  save                   Save current configuration
  security-logfile       Security log file configuration
  service-instance       Configure a service instance
  sflow                  sFlow function
  shutdown               Shut down the interface
  smart-link             Smart Link module
  spbm                   SPBM configuration
  speed                  Specify speed of current port
  storm-constrain        Port storm control
  stp                    Spanning Tree Protocol (STP) module
  tracert                Tracert function
  trill                  TRansparent Interconnection of Lots of Links (TRILL)
                         module
  undo                   Cancel current setting
  unicast-suppression    Unicast storm suppression function
  virtual-cable-test     Test cable connection for an interface
  vlan                   Set VLAN precedence
  voice-vlan             Voice VLAN configuration

[Comware7-GigabitEthernet1/0/6]port ?
  access            Set access port attributes
  auto-power-down   Auto power down an idle interface
  bridge            Configure bridging
  hybrid            Set hybrid port attributes
  link-aggregation  Link aggregation group
  link-mode         Switch the specified interface to layer2 or layer3 ethernet
  link-type         Set the link type
  monitor-link      Monitor Link module
  multicast-vlan    Specify a multicast VLAN
  private-vlan      Private VLAN function
  pvid              Forward packets within the PVID
  service-loopback  Service loop back group
  smart-link        Smart Link module
  trunk             Set trunk port attributes
  up-mode           Forcibly bring up an interface without a fiber connection

[Comware7-GigabitEthernet1/0/6]port link-type ?
  access  Set the link type to access
  hybrid  Set the link type to hybrid
  trunk   Set the link type to trunk

[Comware7-GigabitEthernet1/0/6]port link-type trunk

[Comware7-GigabitEthernet1/0/6]port trunk ?
  permit  Assign the port to VLANs
  pvid    Specify the port PVID

[Comware7-GigabitEthernet1/0/6]port trunk permit ?
  vlan  Specify permitted VLANs

[Comware7-GigabitEthernet1/0/6]port trunk permit vlan ?
  INTEGER<1-4094>  VLAN ID
  all              All VLANs
```

```
[Comware7-GigabitEthernet1/0/6]port trunk permit vlan 100 220


[Comware7]vlan 220

[Comware7-vlan220]?
Vlan view commands:
  arp                     ARP module
  cfd                     Connectivity Fault Detection (CFD) module
  description             Configure the VLAN description
  diagnostic-logfile      Diagnostic log file configuration
  display                 Display current system information
  igmp-snooping           IGMP snooping module
  ip-subnet-vlan
  ipv6                    Specify IPv6 configuration
  logfile                 Log file configuration
  mac-address             Configure MAC address
  mac-forced-forwarding   Specify MAC-forced forwarding configuration information
  mld-snooping            MLD snooping module
  monitor                 System monitor
  name                    Configure the VLAN name
  pim-snooping            PIM snooping module
  ping                    Ping function
  port                    Assign ports to or remove ports from the VLAN
  private-vlan            Private VLAN function
  protocol-vlan           Protocol-based VLAN
  quit                    Exit from current command view
  return                  Exit to User View
  save                    Save current configuration
  security-logfile        Security log file configuration
  subvlan                 Specify sub-VLAN
  supervlan               Specify the VLAN as a super VLAN
  tracert                 Tracert function
  undo                    Cancel current setting

[Comware7-vlan220]port ?
  FortyGigE             FortyGigE interface
  GigabitEthernet       GigabitEthernet interface
  Ten-GigabitEthernet   Ten-GigabitEthernet interface

[Comware7-vlan220]port g1/0/4 ?
  FortyGigE             FortyGigE interface
  GigabitEthernet       GigabitEthernet interface
  Ten-GigabitEthernet   Ten-GigabitEthernet interface
  to                    Range of interfaces
  <cr>

[Comware7-vlan220]port g1/0/4


[Comware7]display vlan 220
VLAN ID: 220
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0220
 Name: test
 Tagged ports:
    GigabitEthernet1/0/6
 Untagged ports:
    GigabitEthernet1/0/4

[Comware7]display vlan 100
```

```
VLAN ID: 100
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged ports:
    GigabitEthernet1/0/6
 Untagged ports:
    GigabitEthernet1/0/5          GigabitEthernet1/0/9

[Comware7]display vlan 1
 VLAN ID: 1
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 10.0.111.51
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports:
    FortyGigE1/0/53               FortyGigE1/0/54
    GigabitEthernet1/0/1          GigabitEthernet1/0/2
    GigabitEthernet1/0/3          GigabitEthernet1/0/6
    GigabitEthernet1/0/7          GigabitEthernet1/0/8
    GigabitEthernet1/0/10         GigabitEthernet1/0/11
    GigabitEthernet1/0/12         GigabitEthernet1/0/13
    GigabitEthernet1/0/14         GigabitEthernet1/0/15
    GigabitEthernet1/0/16         GigabitEthernet1/0/17
    GigabitEthernet1/0/18         GigabitEthernet1/0/19
    GigabitEthernet1/0/20         GigabitEthernet1/0/21
    GigabitEthernet1/0/22         GigabitEthernet1/0/23
    GigabitEthernet1/0/24         GigabitEthernet1/0/25
    GigabitEthernet1/0/26         GigabitEthernet1/0/27
    GigabitEthernet1/0/28         GigabitEthernet1/0/29
    GigabitEthernet1/0/30         GigabitEthernet1/0/31
    GigabitEthernet1/0/32         GigabitEthernet1/0/33
    GigabitEthernet1/0/34         GigabitEthernet1/0/35
    GigabitEthernet1/0/36         GigabitEthernet1/0/37
    GigabitEthernet1/0/38         GigabitEthernet1/0/39
    GigabitEthernet1/0/40         GigabitEthernet1/0/41
    GigabitEthernet1/0/42         GigabitEthernet1/0/43
    GigabitEthernet1/0/44         GigabitEthernet1/0/45
    GigabitEthernet1/0/46         GigabitEthernet1/0/47
    GigabitEthernet1/0/48
    Ten-GigabitEthernet1/0/49
    Ten-GigabitEthernet1/0/50
    Ten-GigabitEthernet1/0/51
    Ten-GigabitEthernet1/0/52


[Comware7]display interface g1/0/6
GigabitEthernet1/0/6
Current state: UP
Line protocol state: UP
IP packet frame type: Ethernet II, hardware address: cc3e-5f73-baf9
Description: GigabitEthernet1/0/6 Interface
Bandwidth: 1000000 kbps
Loopback is not set
Media type is twisted pair
Port hardware type is 1000_BASE_T
1000Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
```

```
Maximum frame length: 10000
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
PVID: 1
MDI type: automdix
Port link-type: Trunk
 VLAN Passing:   1(default vlan), 100, 220
 VLAN permitted: 1(default vlan), 100, 220
 Trunk port encapsulation: IEEE 802.1q
Port priority: 0
Last clearing of counters: Never
 Peak input rate: 5 bytes/sec, at 2015-04-08 02:03:03
 Peak output rate: 8 bytes/sec, at 2015-04-08 02:03:03
 Last 300 second input: 0 packets/sec 5 bytes/sec 0%
 Last 300 second output: 0 packets/sec 8 bytes/sec 0%
 Input (total):  17 packets, 1801 bytes
         4 unicasts, 5 broadcasts, 8 multicasts, 0 pauses
 Input (normal):  17 packets, - bytes
         4 unicasts, 5 broadcasts, 8 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
 Output (total): 16 packets, 2626 bytes
         3 unicasts, 6 broadcasts, 7 multicasts, 0 pauses
 Output (normal): 16 packets, - bytes
         3 unicasts, 6 broadcasts, 7 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier


[Comware7]display interface g1/0/5
GigabitEthernet1/0/5
Current state: DOWN
Line protocol state: DOWN
IP packet frame type: Ethernet II, hardware address: cc3e-5f73-baf8
Description: GigabitEthernet1/0/5 Interface
Bandwidth: 1000000 kbps
Loopback is not set
Media type is twisted pair
Port hardware type is 1000_BASE_T
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 10000
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
PVID: 100
MDI type: automdix
Port link-type: Access
 Tagged VLANs:   None
 Untagged VLANs: 100
Port priority: 0
Last clearing of counters: Never
 Peak input rate: 0 bytes/sec, at 2010-12-31 18:01:19
 Peak output rate: 0 bytes/sec, at 2010-12-31 18:01:19
 Last 300 second input: 0 packets/sec 0 bytes/sec -%
 Last 300 second output: 0 packets/sec 0 bytes/sec -%
 Input (total):  0 packets, 0 bytes
```

```
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input (normal):  0 packets, - bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
 Output (total): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 0 packets, - bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier
```

Cisco

```
Cisco(config)#interface g1/0/6

Cisco(config-if)#?
Interface configuration commands:
  aaa                      Authentication, Authorization and Accounting.
  arp                      Set arp type (arpa, probe, snap) or timeout or log
                           options
  auto                     Configure Automation
  bandwidth                Set bandwidth informational parameter
  bgp-policy               Apply policy propagated by bgp community string
  carrier-delay            Specify delay for interface transitions
  cdp                      CDP interface subcommands
  channel-group            Etherchannel/port bundling configuration
  channel-protocol         Select the channel protocol (LACP, PAgP)
  cts                      Configure Cisco Trusted Security
  dampening                Enable event dampening
  datalink                 Interface Datalink commands
  default                  Set a command to its defaults
  delay                    Specify interface throughput delay
  description              Interface specific description
  down-when-looped         Force looped interface down
  duplex                   Configure duplex operation.
  eou                      EAPoUDP Interface Configuration Commands
  exit                     Exit from interface configuration mode
  flow-sampler             Attach flow sampler to the interface
  flowcontrol              Configure flow operation.
  help                     Description of the interactive help system
  history                  Interface history histograms - 60 second, 60 minute
                           and 72 hour
  hold-queue               Set hold queue depth
  ip                       Interface Internet Protocol config commands
  keepalive                Enable keepalive
  l2protocol-tunnel        Tunnel Layer2 protocols
  lacp                     LACP interface subcommands
  link                     Configure Link
  lldp                     LLDP interface subcommands
  load-interval            Specify interval for load calculation for an
                           interface
  location                 Interface location information
  logging                  Configure logging for interface
  mac                      MAC interface commands
  macro                    Command macro
  max-reserved-bandwidth   Maximum Reservable Bandwidth on an Interface
  mdix                     Set Media Dependent Interface with Crossover
  mka                      MACsec Key Agreement (MKA) interface configuration
  mls                      mls interface commands
  mvr                      MVR per port configuration
  neighbor                 interface neighbor configuration mode commands
```

```
  network-policy          Network Policy
  nmsp                    NMSP interface configuration
  no                      Negate a command or set its defaults
  pagp                    PAgP interface subcommands
  priority-queue          Priority Queue
  queue-set               Choose a queue set for this queue
  rmon                    Configure Remote Monitoring on an interface
  routing                 Per-interface routing configuration
  rsu                     rollsing stack upgrade
  service-policy          Configure CPL Service Policy
  shutdown                Shutdown the selected interface
  small-frame             Set rate limit parameters for small frame
  snmp                    Modify SNMP interface parameters
  source                  Get config from another source
  spanning-tree           Spanning Tree Subsystem
  speed                   Configure speed operation.
  srr-queue               Configure shaped round-robin transmit queues
  storm-control           storm configuration
  switchport              Set switching mode characteristics
  timeout                 Define timeout values for this interface
  topology                Configure routing topology on the interface
  transmit-interface      Assign a transmit interface to a receive-only
                          interface
  tx-ring-limit           Configure PA level transmit ring limit
  udld                    Configure UDLD enabled or disabled and ignore global
                          UDLD setting
  vtp                     Enable VTP on this interface

Cisco(config-if)#switchport ?
  access         Set access mode characteristics of the interface
  autostate      Include or exclude this port from vlan link up calculation
  backup         Set backup for the interface
  block          Disable forwarding of unknown uni/multi cast addresses
  host           Set port host
  mode           Set trunking mode of the interface
  nonegotiate    Device will not engage in negotiation protocol on this
                 interface
  port-security  Security related command
  priority       Set appliance 802.1p priority
  private-vlan   Set the private VLAN configuration
  protected      Configure an interface to be a protected port
  trunk          Set trunking characteristics of the interface
  voice          Voice appliance attributes
  <cr>

Cisco(config-if)#switchport trunk ?
  allowed        Set allowed VLAN characteristics when interface is in trunking
                 mode
  encapsulation  Set trunking encapsulation when interface is in trunking mode
  native         Set trunking native characteristics when interface is in
                 trunking mode
  pruning        Set pruning VLAN characteristics when interface is in trunking
                 mode

Cisco(config-if)#switchport trunk encapsulation ?
  dot1q      Interface uses only 802.1q trunking encapsulation when trunking
  isl        Interface uses only ISL trunking encapsulation when trunking
  negotiate  Device will negotiate trunking encapsulation with peer on
             interface

Cisco(config-if)#switchport trunk encapsulation dot1q
```

```
Cisco(config-if)#switchport trunk allowed ?
  vlan  Set allowed VLANs when interface is in trunking mode

Cisco(config-if)#switchport trunk allowed vlan ?
  WORD    VLAN IDs of the allowed VLANs when this port is in trunking mode
  add     add VLANs to the current list
  all     all VLANs
  except  all VLANs except the following
  none    no VLANs
  remove  remove VLANs from the current list

Cisco(config-if)#switchport trunk allowed vlan 100 ?
  <cr>

Cisco(config-if)#switchport trunk allowed vlan 100,?
WORD

Cisco(config-if)#switchport trunk allowed vlan 100,220


Cisco(config-if)#switchport mode ?
  access        Set trunking mode to ACCESS unconditionally
  dot1q-tunnel  set trunking mode to TUNNEL unconditionally
  dynamic       Set trunking mode to dynamically negotiate access or trunk mode
  private-vlan  Set private-vlan mode
  trunk         Set trunking mode to TRUNK unconditionally

Cisco(config-if)#switchport mode trunk


Cisco(config-if)#switchport nonegotiate


Cisco(config)#interface g1/0/4

Cisco(config-if)#switchport

Cisco(config-if)#switchport access vlan 220

Cisco(config-if)#switchport mode access


Cisco#show vlan id 220

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
220  test                             active    Gi1/0/4, Gi1/0/6

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
220  enet  100220     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------


Cisco#show vlan id 100

VLAN Name                             Status    Ports
```

```
---- -------------------------------- --------- -------------------------------
100  VLAN0100                         active    Gi1/0/5, Gi1/0/6, Gi1/0/9

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
100  enet  100100     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ----------------------------------------


Cisco#show vlan id 1

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                                                Gi1/0/7, Gi1/0/8, Gi1/0/10
                                                Gi1/0/11, Gi1/0/12, Gi1/0/13
                                                Gi1/0/14, Gi1/0/15, Gi1/0/16
                                                Gi1/0/17, Gi1/0/18, Gi1/0/19
                                                Gi1/0/20, Gi1/0/21, Gi1/0/22
                                                Gi1/0/23, Gi1/0/24, Te1/0/1
                                                Te1/0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ----------------------------------------

Cisco#show interfaces g1/0/6 switchport
Name: Gi1/0/6
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 100 (VLAN0100)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 100,220
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

```
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

Cisco#show interfaces g1/0/5 switchport
Name: Gi1/0/5
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: Off
Access Mode VLAN: 100 (VLAN0100)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

c) Assigning an IP Address to a VLAN

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# vlan 220	[Comware]interface Vlan-interface 220	Cisco(config)#interface vlan 220
ArubaOS-Switch(vlan-220)# ip address 10.1.220.1/24	[Comware-Vlan-interface220]ip address 10.1.220.3 24	Cisco(config-if)#ip address 10.1.220.2 255.255.255.0
		Cisco(config-if)#no shutdown
ArubaOS-Switch# show ip	[Comware]display ip interface brief	Cisco#show ip interface brief

ArubaOS-Switch

```
ArubaOS-Switch(config)# vlan 220

ArubaOS-Switch(vlan-220)# ip address 10.1.220.1/24
```

-or-

```
ArubaOS-Switch(vlan-220)# ip address 10.1.220.1 255.255.255.0


ArubaOS-Switch# show ip

 Internet (IP) Service

  IP Routing : Enabled


  Default TTL      : 64
  Arp Age          : 20
  Domain Suffix    :
  DNS server       : 74.82.42.42

                        |                                                Proxy ARP
  VLAN                  | IP Config  IP Address      Subnet Mask     Std  Local
  -------------------- + ---------- --------------- --------------- ----------
  DEFAULT_VLAN          | Manual     10.0.111.21     255.255.255.0    No    No
  VLAN100               | Disabled
  test                  | Manual     10.1.220.1      255.255.255.0    No    No
  test2                 | Disabled
```

Comware

```
[Comware]interface Vlan-interface 220

[Comware-Vlan-interface220]ip address 10.1.220.3 ?
  INTEGER<1-31>  IP mask length
  X.X.X.X        IP mask

[Comware-Vlan-interface220]ip address 10.1.220.3 24
```

-or-

```
[Comware-Vlan-interface220]ip address 10.1.220.3 255.255.255.0


[Comware]display ip interface brief
*down: administratively down
(s): spoofing
Interface                      Physical Protocol IP Address      Description
```

```
Vlan1                          up       up       10.0.111.31     Vlan-inte...
Vlan220                        up       up       10.1.220.3      Vlan-inte...
```

Cisco

```
Cisco(config)#interface vlan 220

Cisco(config-if)#ip address 10.1.220.4 255.255.255.0


Cisco(config-if)#no shutdown


Cisco#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  10.0.111.41     YES NVRAM  up                    up
Vlan220                10.1.220.4      YES manual up                    up
FastEthernet0          unassigned      YES NVRAM  administratively down down
GigabitEthernet1/0/1   unassigned      YES unset  up                    up
GigabitEthernet1/0/2   unassigned      YES unset  down                  down
GigabitEthernet1/0/3   unassigned      YES unset  down                  down
GigabitEthernet1/0/4   unassigned      YES unset  down                  down
GigabitEthernet1/0/5   unassigned      YES unset  down                  down
GigabitEthernet1/0/6   unassigned      YES unset  up                    up
GigabitEthernet1/0/7   unassigned      YES unset  down                  down
GigabitEthernet1/0/8   unassigned      YES unset  down                  down
GigabitEthernet1/0/9   unassigned      YES unset  down                  down
GigabitEthernet1/0/10  unassigned      YES unset  down                  down
GigabitEthernet1/0/11  unassigned      YES unset  down                  down
GigabitEthernet1/0/12  unassigned      YES unset  down                  down
GigabitEthernet1/0/13  unassigned      YES unset  down                  down
GigabitEthernet1/0/14  unassigned      YES unset  down                  down
GigabitEthernet1/0/15  unassigned      YES unset  down                  down
GigabitEthernet1/0/16  unassigned      YES unset  down                  down
GigabitEthernet1/0/17  unassigned      YES unset  down                  down
GigabitEthernet1/0/18  unassigned      YES unset  down                  down
GigabitEthernet1/0/19  unassigned      YES unset  down                  down
GigabitEthernet1/0/20  unassigned      YES unset  down                  down
GigabitEthernet1/0/21  unassigned      YES unset  down                  down
GigabitEthernet1/0/22  unassigned      YES unset  down                  down
GigabitEthernet1/0/23  unassigned      YES unset  down                  down
GigabitEthernet1/0/24  unassigned      YES unset  down                  down
GigabitEthernet1/0/25  unassigned      YES unset  down                  down
GigabitEthernet1/0/26  unassigned      YES unset  down                  down
GigabitEthernet1/0/27  unassigned      YES unset  down                  down
GigabitEthernet1/0/28  unassigned      YES unset  down                  down
Te1/0/1                unassigned      YES unset  down                  down
Te1/0/2                unassigned      YES unset  down                  down
```

d) IP Helper to Relay / Forward DHCP Requests

ArubaOS-Switch	Comware5	Cisco
ArubaOS-Switch(config)# vlan 220		Cisco(config)#interface vlan 220
ArubaOS-Switch(vlan-220)# ip helper-address 10.0.100.251		Cisco(config-if)#ip helper-address 10.0.100.251
	[Comware5]dhcp enable	
	[Comware5]dhcp relay server-group 1 ip 10.0.100.251	
	[Comware5]interface Vlan-interface 220	
	[Comware5-Vlan-interface220]dhcp select relay	
	[Comware5-Vlan-interface220]dhcp relay server-select 1	
ArubaOS-Switch# show ip helper-address vlan 220	[Comware5]display dhcp relay all	Cisco#show ip interface vlan 220
ArubaOS-Switch# show dhcp-relay	[Comware5]display dhcp relay server-group 1	
	Comware7	
	[Comware7]dhcp enable	
	[Comware7]interface Vlan-interface 220	
	[Comware7-Vlan-interface220]dhcp select relay	
	[Comware7-Vlan-interface220]dhcp relay server-address 10.0.100.251	
	[Comware7]display dhcp relay server-address	
	[Comware7]display dhcp relay statistics interface Vlan-interface 220	

ArubaOS-Switch

```
ArubaOS-Switch(config)# vlan 220

ArubaOS-Switch(vlan-220)# ip helper-address 10.0.100.251
```

(also as compound statement)

```
ArubaOS-Switch(config)# vlan 220 ip helper-address 10.0.100.251


ArubaOS-Switch(vlan-220)# show ip helper-address vlan 220

 IP Helper Addresses

  IP Helper Address
  -----------------
  10.0.100.251
```

```
ArubaOS-Switch# show dhcp-relay
  DHCP Relay Agent                  : Enabled
  DHCP Request Hop Count Increment : Enabled
  Option 82                         : Disabled
  Response validation               : Disabled
  Option 82 handle policy           : replace
  Remote ID                         : mac

  DHCP Relay Statistics:

  Client Requests       Server Responses

  Valid      Dropped    Valid      Dropped
  ---------- ---------- ---------- ----------
  17         0          6          0

  DHCP Relay Option 82 Statistics:

  Client Requests       Server Responses

  Valid      Dropped    Valid      Dropped
  ---------- ---------- ---------- ----------
  0          0          0          0
```

Comware5

```
[Comware5]dhcp ?
  client  DHCP client configuration subcommands
  dscp    Specify the DSCP value in DHCP/BOOTP client packet
  enable  DHCP service enable
  relay   Specify DHCP(Dynamic Host Configuration Protocol) relay configuration
          information
  server  DHCP server

[Comware5]dhcp enable
 DHCP is enabled successfully!

[Comware5]dhcp relay ?
  release        Release one IP address
  security       Specify DHCP(Dynamic Host Configuration Protocol) relay
                 security configuration information
  server-detect  Detect fake DHCP server
  server-group   Specify the server group number

[Comware5]dhcp relay server-group ?
  INTEGER<0-19>  The DHCP server group number

[Comware5]dhcp relay server-group 1 ?
  ip  Specify DHCP server IP address

[Comware5]dhcp relay server-group 1 ip ?
  X.X.X.X  The IP address of the DHCP server

[Comware5]dhcp relay server-group 1 ip 10.0.100.251 ?
  <cr>

[Comware5]dhcp relay server-group 1 ip 10.0.100.251


[Comware5]interface Vlan-interface 220

[Comware5-Vlan-interface220]dhcp ?
  relay   Specify DHCP(Dynamic Host Configuration Protocol) relay configuration
```

```
          information
  select  Specify process mode of DHCP packet
  server  DHCP server

[Comware5-Vlan-interface220]dhcp select ?
  relay   Relay mode
  server  Server mode

[Comware5-Vlan-interface220]dhcp select relay ?
  <cr>

[Comware5-Vlan-interface220]dhcp select relay

[Comware5-Vlan-interface220]dhcp relay ?
  address-check  Check address
  check          Check the DHCP packet
  client-detect  Detect off-line client through ARP entries
  information    Specify option 82 service
  server-select  Choose DHCP server group

[Comware5-Vlan-interface220]dhcp relay server-select ?
  INTEGER<0-19>  The DHCP server group number

[Comware5-Vlan-interface220]dhcp relay server-select 1 ?
  <cr>

[Comware5-Vlan-interface220]dhcp relay server-select 1


[Comware5]display dhcp relay all
    Interface name                                  Server-group
    Vlan-interface220                                     1


[Comware5]display dhcp relay server-group 1
    No.            Group IP
    1              10.0.100.251

[Comware5]display dhcp relay statistics server-group  1
 DHCP relay server-group           #1
     Packet type               Packet number
 Client -> Server:
     DHCPDISCOVER                   119
     DHCPREQUEST                    2
     DHCPINFORM                     2
     DHCPRELEASE                    0
     DHCPDECLINE                    0
     BOOTPREQUEST                   0
 Server -> Client:
     DHCPOFFER                      1
     DHCPACK                        2
     DHCPNAK                        0
     BOOTPREPLY                     0
```

Comware7

```
[Comware7]dhcp ?
  class     Create a DHCP class
  client    Configure a DHCP client
  dscp      Set the Differentiated Services Codepoint (DSCP) value
  enable    Enable DHCP
  relay     Configure a DHCP relay agent
  server    Configure a DHCP server
  snooping  Configure DHCP snooping
```

```
[Comware7]dhcp enable


[Comware7]interface Vlan-interface 220

[Comware7-Vlan-interface220]dhcp ?
  client  Configure a DHCP client
  relay   Configure a DHCP relay agent
  select  Specify process mode of DHCP packet
  server  Configure a DHCP server

[Comware7-Vlan-interface220]dhcp select ?
  relay   Relay mode
  server  Server mode

[Comware7-Vlan-interface220]dhcp select relay ?
  <cr>

[Comware7-Vlan-interface220]dhcp select relay


[Comware7-Vlan-interface220]dhcp relay ?
  check           Check the DHCP packet
  information     DHCP relay agent information
  server-address  Specify the IP address of DHCP server

[Comware7-Vlan-interface220]dhcp relay server-address ?
  X.X.X.X  IP address

[Comware7-Vlan-interface220]dhcp relay server-address 10.0.100.251 ?
  <cr>

[Comware7-Vlan-interface220]dhcp relay server-address 10.0.100.251


[Comware7]display dhcp relay server-address
Interface name                 Server IP address
Vlan220                        10.0.100.251


[Comware7]display dhcp relay statistics interface Vlan-interface 220
DHCP packets dropped:                   0
DHCP packets received from clients:     17
   DHCPDISCOVER:                        10
   DHCPREQUEST:                         3
   DHCPINFORM:                          4
   DHCPRELEASE:                         0
   DHCPDECLINE:                         0
   BOOTPREQUEST:                        0
DHCP packets received from servers:     9
   DHCPOFFER:                           2
   DHCPACK:                             7
   DHCPNAK:                             0
   BOOTPREPLY:                          0
DHCP packets relayed to servers:        17
   DHCPDISCOVER:                        10
   DHCPREQUEST:                         3
   DHCPINFORM:                          4
   DHCPRELEASE:                         0
   DHCPDECLINE:                         0
   BOOTPREQUEST:                        0
DHCP packets relayed to clients:        9
```

```
   DHCPOFFER:                          2
   DHCPACK:                            7
   DHCPNAK:                            0
   BOOTPREPLY:                         0
DHCP packets sent to servers:          0
   DHCPDISCOVER:                       0
   DHCPREQUEST:                        0
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets sent to clients:          0
   DHCPOFFER:                          0
   DHCPACK:                            0
   DHCPNAK:                            0
   BOOTPREPLY:                         0
```

Cisco

```
Cisco(config)#interface vlan 220

Cisco(config-if)#ip ?
Interface IP configuration subcommands:
  access-group        Specify access control for packets
  accounting          Enable IP accounting on this interface
  address             Set the IP address of an interface
  admission           Apply Network Admission Control
  auth-proxy          Apply authenticaton proxy
  authentication      authentication subcommands
  bandwidth-percent   Set EIGRP bandwidth limit
  broadcast-address   Set the broadcast address of an interface
  cef                 Cisco Express Forwarding interface commands
  cgmp                Enable/disable CGMP
  dampening-change    Percent interface metric must change to cause update
  dampening-interval  Time in seconds to check interface metrics
  dhcp                Configure DHCP parameters for this interface
  directed-broadcast  Enable forwarding of directed broadcasts
  flow                NetFlow related commands
  header-compression  IPHC options
  hello-interval      Configures EIGRP-IPv4 hello interval
  helper-address      Specify a destination address for UDP broadcasts
  hold-time           Configures EIGRP-IPv4 hold time
  igmp                IGMP interface commands
  information-reply   Enable sending ICMP Information Reply messages
  irdp                ICMP Router Discovery Protocol
  load-sharing        Style of load sharing
  local-proxy-arp     Enable local-proxy ARP
  mask-reply          Enable sending ICMP Mask Reply messages
  mroute-cache        Enable switching cache for incoming multicast packets
  mtu                 Set IP Maximum Transmission Unit
  multicast           IP multicast interface commands
  next-hop-self       Configures EIGRP-IPv4 next-hop-self
  ospf                OSPF interface commands
  pim                 PIM interface commands
  probe               Enable HP Probe support
  proxy-arp           Enable proxy ARP
  rarp-server         Enable RARP server for static arp entries
  redirects           Enable sending ICMP Redirect messages
```

```
  rgmp                Enable/disable RGMP
  rip                 Router Information Protocol
  route-cache         Enable fast-switching cache for outgoing packets
  rsvp                RSVP Interface Commands
  rtp                 RTP parameters
  sap                 Session Advertisement Protocol interface commands
  security            DDN IP Security Option
  split-horizon       Perform split horizon
  sticky-arp          Allow the creation of sticky ARP entries
  summary-address     Perform address summarization
  tcp                 TCP interface commands
  unnumbered          Enable IP processing without an explicit address
  unreachables        Enable sending ICMP Unreachable messages
  urd                 Configure URL Rendezvousing
  verify              Enable per packet validation

Cisco(config-if)#ip helper-address ?
  A.B.C.D  IP destination address
  global   Helper-address is global
  vrf      VRF name for helper-address (if different from interface VRF)

Cisco(config-if)#ip helper-address 10.0.100.251


Cisco#show ip interface vlan 220
Vlan220 is up, line protocol is up
  Internet address is 10.1.220.4/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 10.0.100.251
  ...
```

Chapter 17 Advanced VLAN Features

This chapter compares the commands that are used to configure advanced VLAN features.

Private VLANs partition an existing VLAN into multiple sets of ports for traffic isolation. The partitioned VLAN is referred to as the Primary VLAN. The sub domains separated from the Primary VLAN are referred to as Secondary VLANs. Secondary VLANs are considered regular VLANs and are identified by using a unique VLAN-ID.

Multiple VLAN Registration Protocol (MVRP) is a registration protocol defined by IEEE, which propagates VLAN information dynamically across devices. It also enables devices to learn and automatically synchronize VLAN configuration information, thereby reducing the configuration workload. It is an enhanced version of GVRP and improves declaration efficiency. It allows a participant (port) to make or withdraw declaration of attributes (VLANs). These declarations (or withdraws) are resulted in registration (or removal of registrations) with other switches in the network.

Virtual eXtensible LAN (VXLAN) is a MAC-in-UDP technology that provides Layer 2 connectivity between distant network sites across an IP network. VXLAN is typically used in data centers for multitenant services.

VXLAN provides the following benefits:
• Support for more virtual switched domains than VLANs—Each VXLAN is uniquely identified by a 24-bit VXLAN ID. The total number of VXLANs can reach 16777216 (224). This specification makes VXLAN a better choice than 802.1Q VLAN to isolate traffic for VMs.
• Easy deployment and maintenance—VXLAN requires deployment only on the edge devices of the transport network. Devices in the transport network perform typical Layer 3 forwarding.

a) Private VLAN

ArubaOS-Switch	Comware7	Cisco
		`Cisco(config)#vtp mode transparent`
`ArubaOS-Switch(config)# vlan 150 private-vlan primary`	`[Comware7]vlan 150`	`Cisco(config)#vlan 150`

	`[Comware7-vlan150]private-vlan primary`
	
	`[Comware7-vlan150]quit`
		`Cisco(config-vlan)#private-vlan primary`
		
		`Cisco(config-vlan)#exit`

`ArubaOS-Switch(config)# vlan 150 private-vlan isolated 151`	`[Comware7]vlan 151`	`Cisco(config)#vlan 151`

	`[Comware7-vlan151]private-vlan isolated`
	
	`[Comware7-vlan151]quit`
		`Cisco(config-vlan)#private-vlan isolated`
		
		`Cisco(config-vlan)#exit`

`ArubaOS-Switch(config)# vlan 150 private-vlan community 152`	`[Comware7]vlan 152`	`Cisco(config)#vlan 152`
	`[Comware7-vlan152]private-vlan community`	`Cisco(config-vlan)#private-vlan community`

	[Comware7-vlan152]quit	Cisco(config-vlan)#exit
	[Comware7]vlan 150	Cisco(config)#vlan 150
	[Comware7-vlan150]private-vlan secondary 151 to 152 [Comware7-vlan150]quit	Cisco(config-vlan)#private-vlan association add 151-152 Cisco(config-vlan)#exit
ArubaOS-Switch(config)# interface 10 private-vlan promiscuous ArubaOS-Switch(config)# vlan 150 untag 10	[Comware7]interface g1/0/10	Cisco(config)#interface g1/0/10
	[Comware7-GigabitEthernet1/0/10]port private-vlan 150 promiscuous	Cisco(config-if)#switchport mode private-vlan promiscuous
		Cisco(config-if)#switchport private-vlan mapping 150 add 151-152
ArubaOS-Switch(config)# vlan 151 untag 12,13	[Comware7-GigabitEthernet1/0/10]interface g1/0/12	Cisco(config)#interface g1/0/12
	[Comware7-GigabitEthernet1/0/12]port private-vlan host	Cisco(config-if)#switchport mode private-vlan host
	[Comware7-GigabitEthernet1/0/12]port access vlan 151	Cisco(config-if)#switchport private-vlan host-association 150 151
ArubaOS-Switch(config)# vlan 152 untag 14,15	[Comware7-GigabitEthernet1/0/12]interface g1/0/14	Cisco(config)#int g1/0/14
	[Comware7-GigabitEthernet1/0/14]port private-vlan host	Cisco(config-if)#switchport mode private-vlan host
	[Comware7-GigabitEthernet1/0/14]port access vlan 152 [Comware7-GigabitEthernet1/0/14]quit	Cisco(config-if)#switchport private-vlan host-association 150 152
ArubaOS-Switch(config)# vlan 150 ip address 10.150.1.1/24	[Comware7]interface vlan 150	Cisco(config)#interface vlan 150
	[Comware7-Vlan-interface150]ip address 10.150.2.1 24	Cisco(config-if)#ip addr 10.150.3.1 255.255.255.0
	[Comware7-Vlan-interface150]private-vlan secondary 151 to 152	Cisco(config-if)#private-vlan mapping add 151-152
ArubaOS-Switch(Vlan-id)#private-vlan primary		Cisco(config)#feature private-vlan
ArubaOS-Switch(Vlan-id)#private-vlan isolated 20		Cisco(config-vlan)# private-vlan isolated
ArubaOS-Switch(Vlan-id)#private-vlan community 3		Cisco(config-vlan)# private-vlan community
ArubaOS-Switch#show private-vlan promiscuous port		Cisco(config-vlan)#show interface switchport
ArubaOS-Switch# show vlans private-vlan	[Comware7]display private-vlan	Cisco#show vlan private-vlan
ArubaOS-Switch# show vlans 150 private-vlan		Cisco#show vlan private-vlan type
		Cisco#show interface private-vlan mapping

ArubaOS-Switch# show vlans 150 ArubaOS-Switch# show vlans 151 ArubaOS-Switch# show vlans 152		

ArubaOS-Switch

```
ArubaOS-Switch(config)# vlan 150 ?
 connection-rate-fi... Reenable access to a host or set of hosts previously blocked by
                       the connection rate filter.
 dhcp-server           Enable the DHCP service on the VLAN.
 dhcp-snooping         Enable DHCP snooping on the VLAN.
 dhcpv6-snooping       Enable DHCPv6 snooping on the VLAN.
 disable               Disable various features on the device.
 forbid                Prevent ports from becoming a member of the current VLAN.
 igmp-proxy            Associate an IGMP proxy domain with a VLAN.
 ip                    Configure various IP parameters for the VLAN.
 ip-recv-mac-address   Associates a L3-mac-address with a VLAN.
 ipv6                  Configure various IPv6 parameters for the VLAN.
 isolate-list          Configure a list of isolated ports for the VLAN.
 jumbo                 Labels this VLAN as a Jumbo VLAN, allowing you to pass packets up
                       to 9216 bytes in size.
 monitor               Define whether the VLAN is to be monitored or not.
 name                  Set the VLAN's name.
 ntp                   Enable/configure NTP operation on the VLAN/OOBM.
 portal                Enable BYOD redirection on this VLAN.
 private-vlan          Configure private VLAN settings.
 protocol              Set a predefined protocol for the current VLAN.
 qos                   Configure VLAN-based traffic prioritization.
 service-policy        Apply a service-policy on the VLAN.
 tagged                Assign ports to current VLAN as tagged.
 untagged              Assign ports to current VLAN as untagged.
 voice                 Labels this VLAN as a Voice VLAN, allowing you to separate,
                       prioritize, and authenticate voice traffic moving through your
                       network.
 vrrp                  Enable/configure VRRP operation on the VLAN.
 <cr>

ArubaOS-Switch(config)# vlan 150 private-vlan ?
 community             Configure the community VLAN IDs for this private VLAN.
 isolated              Configure the isolated VLAN ID for this private VLAN.
 primary               Configure this VLAN as the primary VLAN.

ArubaOS-Switch(config)# vlan 150 private-vlan primary ?
 <cr>

ArubaOS-Switch(config)# vlan 150 private-vlan primary
All primary VLAN ports are automatically configured as trusted for
DHCP Snooping and ND Snooping.

ArubaOS-Switch(config)# vlan 150 private-vlan isolated ?
 VLAN-ID               Enter a VLAN identifier or the VLAN name if configured.

ArubaOS-Switch(config)# vlan 150 private-vlan isolated 151 ?
 <cr>

ArubaOS-Switch(config)# vlan 150 private-vlan isolated 151

ArubaOS-Switch(config)# vlan 150 private-vlan community ?
 [vlan]VLAN-ID-LIST    Enter a list of VLAN identifiers or one VLAN identifier.
```

```
ArubaOS-Switch(config)# vlan 150 private-vlan community 152 ?
 <cr>

ArubaOS-Switch(config)# vlan 150 private-vlan community 152

ArubaOS-Switch(config)# interface 10 ?
 arp-protect           Configure the port as trusted or untrusted.
 bandwidth-min         Configure guaranteed minimum bandwidth settings.
 broadcast-limit       Limit network bandwidth used by broadcast traffic.
 dhcp-snooping         Configure port-specific DHCP snooping parameters.
 dhcpv6-snooping       Configure DHCPv6 snooping on the port.
 disable               Disable the port.
 dldp                  Enable or disable the Device Link Detection Protocol (DLDP) to
                       monitor link status.
 enable                Enable the port.
 energy-efficient-e... Enable energy-efficient-ethernet on the port.
 flow-control          Enable flow control negotiation on the port during link
                       establishment.
 forbid                Prevent this port from becoming a member of the specified VLAN(s).
 gvrp                  Set the GVRP timers for the port.
 ignore-untagged-mac
 ip                    Apply the specified IPv4 ACL to inbound or outbound packets on
                       this interface.
 ipv6                  Configure various IPv6 parameters for the VLAN.
 lacp                  Define whether LACP is enabled on the port, and whether it is in
                       active or passive mode when enabled.
 link-keepalive        Configure UniDirectional Link Detection (UDLD) on the port.
 mac-count-notify      Send a trap when the number of MAC addresses learned on the
                       specified ports exceeds the threshold.
 mac-notify            Configure SNMP traps for changes in the MAC address table.
 mdix-mode             Set port MDI/MDIX mode (default: auto).
 monitor               Monitor traffic on the port.
 mvrp                  Configure the Multiple VLAN Registration Protocol (MVRP).
 name                  Assign an interface name.
 poe-allocate-by       Configure the power allocation method.
 poe-lldp-detect       Allow the link partner to specify power allocation using LLDP.
 poe-value             Set the maximum power allocation for the port.
 power-over-ethernet   Enable per-port power distribution.
 private-vlan          Configure ports as promiscuous members of private VLANs.
 qos                   Configure port-based traffic prioritization.
 rate-limit            Enable rate limiting for various types of traffic.
 service-policy        Apply a service-policy on the interface.
 smart-link            Configure the control VLANs for receiving flush packets.
 speed-duplex          Define mode of operation for the port(s).
 tagged                Configure this port as a tagged member of the specified VLAN(s).
 unknown-vlans         Configure the GVRP mode.
 untagged              Configure this port as an untagged member of the specified VLAN.
 <cr>
ArubaOS-Switch(config)# interface 10 private-vlan ?
 promiscuous           Configure ports as promiscuous ports.

ArubaOS-Switch(config)# interface 10 private-vlan promiscuous ?
 <cr>
ArubaOS-Switch(config)# interface 10 private-vlan promiscuous

ArubaOS-Switch(config)# vlan 150 untag 10
Ports 10 automatically configured as trusted for DHCP Snooping and
ND Snooping because they are members of a primary VLAN.

ArubaOS-Switch(config)# vlan 151 untag 12,13

ArubaOS-Switch(config)# vlan 152 untag 14,15
```

```
ArubaOS-Switch(config)# vlan 150 ip address 10.150.1.1/24



ArubaOS-Switch# show vlans ?
 custom                Show VLAN parameters in a customized order.
 isolate-list          Show the isolated ports configuration.
 ports                 Show VLANs that have a port from specified list as a member.
 private-vlan          Show VLAN parameters in a customized order.
 VLAN-ID               Show detailed information for a single VLAN.
 <cr>

ArubaOS-Switch# show vlans private-vlan ?
 <cr>

ArubaOS-Switch# show vlans private-vlan

 Configuration and Association â€" private VLANs:

  primary  secondary  VLAN Type
  -------  ---------  ---------
  150      151        isolated
           152        community

ArubaOS-Switch# show vlans 150 ?
 private-vlan          Show VLAN parameters in a customized order.
 <cr>

ArubaOS-Switch# show vlans 150 private-vlan ?
 <cr>

ArubaOS-Switch# show vlans 150 private-vlan

  Private VLAN Configuration Information : VLAN 150


   VLAN Type  : primary

   Port Type          Ports
   ------------------ ---------------------------------------------------
   Promiscuous        10

   Member

  Associated Secondary VLANs:

  VLAN ID    VLAN Type     Access Ports
  ---------- ------------- ---------------------------------------------------
  151        isolated      12-13
  152        community     14-15

ArubaOS-Switch# show private-vlan promiscuous-ports ?
 <cr>

ArubaOS-Switch# show private-vlan promiscuous-ports
 primary VLAN    Port
 --------------- ---------------------------------------------------
 150             10

ArubaOS-Switch# show vlans 150

 Status and Counters - VLAN Information - VLAN 150
```

```
  VLAN ID : 150
  Name : VLAN150
  Status : Port-based
  Voice : No
  Jumbo : No
  Private VLAN : primary
  Associated Primary VID : none
  Associated Secondary VIDs : 151-152

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  10               Untagged Learn        Up

ArubaOS-Switch# show vlans 151

 Status and Counters - VLAN Information - VLAN 151

  VLAN ID : 151
  Name : VLAN151
  Status : Port-based
  Voice : No
  Jumbo : No
  Private VLAN : isolated
  Associated Primary VID : 150
  Associated Secondary VIDs : none

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  12               Untagged Learn        Up
  13               Untagged Learn        Up

ArubaOS-Switch# show vlans 152

 Status and Counters - VLAN Information - VLAN 152

  VLAN ID : 152
  Name : VLAN152
  Status : Port-based
  Voice : No
  Jumbo : No
  Private VLAN : community
  Associated Primary VID : 150
  Associated Secondary VIDs : none

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  14               Untagged Learn        Up
  15               Untagged Learn        Up

ArubaOS-Switch(config)#mdns
<tab>
   default              Set the action of the mDNS default filter.

   disable              Enable or disable mDNS feature.

   enable            Enable or disable mDNS feature.

   gateway           Enable VLAN for mDNS gateway.

   profile           Create or delete an mDNS profile.
```

Comware5

```
Not an available feature.
```

Comware7

```
[Comware7]vlan 150

[Comware7-vlan150]?
Vlan view commands:
  arp                     ARP module
  cfd                     Connectivity Fault Detection (CFD) module
  description             Configure the VLAN description
  diagnostic-logfile      Diagnostic log file configuration
  display                 Display current system information
  igmp-snooping           IGMP snooping module
  ip                      Specify IP configuration
  ip-subnet-vlan
  ipv6                    Specify IPv6 configuration
  logfile                 Log file configuration
  mac-address             Configure MAC address
  mac-forced-forwarding   Specify MAC-forced forwarding configuration information
  mld-snooping            MLD snooping module
  monitor                 System monitor
  name                    Configure the VLAN name
  pim-snooping            PIM snooping module
  ping                    Ping function
  port                    Assign ports to or remove ports from the VLAN
  private-vlan            Private VLAN function
  protocol-vlan           Protocol-based VLAN
  quit                    Exit from current command view
  return                  Exit to User View
  save                    Save current configuration
  security-logfile        Security log file configuration
  subvlan                 Specify sub-VLAN
  supervlan               Specify the VLAN as a super VLAN
  tracert                 Tracert function
  undo                    Cancel current setting

 [Comware7-vlan150]private-vlan ?
  community  Configure the VLAN as a community VLAN
  isolated   Configure the VLAN as an isolated VLAN
  primary    Configure the VLAN as a primary VLAN
  secondary  Specify the secondary VLANs

[Comware7-vlan150]private-vlan primary ?
  <cr>

[Comware7-vlan150]private-vlan primary

[Comware7-vlan150]quit

[Comware7]vlan 151

[Comware7-vlan151]private-vlan ?
  community  Configure the VLAN as a community VLAN
  isolated   Configure the VLAN as an isolated VLAN
  primary    Configure the VLAN as a primary VLAN
  secondary  Specify the secondary VLANs

[Comware7-vlan151]private-vlan isolated ?
  <cr>
```

```
[Comware7-vlan151]private-vlan isolated

[Comware7-vlan151]quit

[Comware7]vlan 152

[Comware7-vlan152]private-vlan ?
  community  Configure the VLAN as a community VLAN
  isolated   Configure the VLAN as an isolated VLAN
  primary    Configure the VLAN as a primary VLAN
  secondary  Specify the secondary VLANs

[Comware7-vlan152]private-vlan community ?
  <cr>

[Comware7-vlan152]private-vlan community

[Comware7-vlan152]quit

[Comware7]vlan 150

[Comware7-vlan150]private-vlan ?
  community  Configure the VLAN as a community VLAN
  isolated   Configure the VLAN as an isolated VLAN
  primary    Configure the VLAN as a primary VLAN
  secondary  Specify the secondary VLANs

[Comware7-vlan150]private-vlan secondary ?
  INTEGER<1-4094>  Secondary VLAN ID

[Comware7-vlan150]private-vlan secondary 151 to 152 ?
  INTEGER<1-4094>  Secondary VLAN ID
  <cr>

[Comware7-vlan150]private-vlan secondary 151 to 152

[Comware7-vlan150]quit

[Comware7]interface g1/0/10

[Comware7-GigabitEthernet1/0/10]?
Gigabitethernet_l2 interface view commands:
  apply                  Apply a PoE profile
  arp                    ARP module
  bandwidth              Specify the expected bandwidth
  bpdu-drop              Specify BPDU drop function
  broadcast-suppression  Broadcast storm suppression function
  cdp                    Non standard IEEE discovery protocol
  cfd                    Connectivity Fault Detection (CFD) module
  dcbx                   Data Center Bridge Capability Exchange Protocol
  default                Restore the default settings
  description            Describe the interface
  dhcp                   DHCP module
  diagnostic-logfile     Diagnostic log file configuration
  display                Display current system information
  dldp                   DLDP module
  dot1x                  802.1X module
  duplex                 Status of duplex
  eee                    Energy efficient ethernet
  enable                 Enable functions
  evb                    Edge Virtual Bridging (EVB) module
  flex10                 Configure Flex10
```

```
flow-control            Enable flow control function
flow-interval           Set the interface statistics interval
igmp-snooping           IGMP snooping module
ip                      Specify IP configuration
ipv6                    Specify IPv6 configuration
jumboframe              Specify jumbo frame forwarding
l2vpn                   Layer 2 Virtual Private Network (L2VPN) module
lacp                    Configure LACP protocol
link-aggregation        Specify link aggregation group configuration
                        information
link-delay              Set the physical state change suppression
lldp                    Link Layer Discovery Protocol(802.1ab)
logfile                 Log file configuration
loopback                Specify loopback of current port
loopback-detection      Loopback detection module
mac-address             Configure MAC address
mac-authentication      MAC authentication module
mac-forced-forwarding   Specify MAC-forced forwarding configuration information
mac-vlan                MAC VLAN configuration
macsec                  MAC security module
mdix-mode               Specify mdix type
mirroring-group         Specify mirroring group
mka                     MACsec Key Agreement protocol
mld-snooping            MLD snooping module
monitor                 System monitor
mrp                     Multiple registration protocol
multicast-suppression   Multicast storm suppression function
mvrp                    Multiple VLAN registration protocol
oam                     OAM module
packet-filter           Packet filter settings
pbb                     Provider Backbone Bridge (PBB) module
ping                    Ping function
poe                     Power over Ethernet
port                    Set port attributes
port-isolate            Port isolation configuration
port-security           Port security module
priority-flow-control   Priority-based flow control (PFC) configuration
ptp                     Precision Time Protocol (PTP) module
qcn                     Quantized Congestion Notification (QCN) module
qinq                    802.1QinQ function
qos                     Quality of Service (QoS) module
quit                    Exit from current command view
return                  Exit to User View
rmon                    RMON module
save                    Save current configuration
security-logfile        Security log file configuration
service-instance        Configure a service instance
sflow                   sFlow function
shutdown                Shut down the interface
smart-link              Smart Link module
spbm                    SPBM configuration
speed                   Specify speed of current port
storm-constrain         Port storm control
stp                     Spanning Tree Protocol (STP) module
tracert                 Tracert function
trill                   TRansparent Interconnection of Lots of Links (TRILL)
                        module
undo                    Cancel current setting
unicast-suppression     Unicast storm suppression function
virtual-cable-test      Test cable connection for an interface
vlan                    Set VLAN precedence
voice-vlan              Voice VLAN configuration
```

```
[Comware7-GigabitEthernet1/0/10]port ?
  access                Set access port attributes
  auto-power-down       Auto power down an idle interface
  bridge                Configure bridging
  connection-distance   Specify the connection distance of the interface
  hybrid                Set hybrid port attributes
  link-aggregation      Link aggregation group
  link-mode             Switch the specified interface to layer2 or layer3
                        ethernet
  link-type             Set the link type
  monitor-link          Monitor Link module
  multicast-vlan        Specify a multicast VLAN
  private-vlan          Private VLAN function
  pvid                  Forward packets within the PVID
  service-loopback      Service loop back group
  smart-link            Smart Link module
  trunk                 Set trunk port attributes
  up-mode               Forcibly bring up an interface without a fiber connection

[Comware7-GigabitEthernet1/0/10]port private-vlan ?
  INTEGER<1-4094>  VLAN ID
  host             Specify the host mode in private VLAN

[Comware7-GigabitEthernet1/0/10]port private-vlan 150 ?
  INTEGER<1-4094>  VLAN ID
  promiscuous      Specify the promiscuous mode in private VLAN
  to               Range of VLAN IDs
  trunk            Specify trunk mode

[Comware7-GigabitEthernet1/0/10]port private-vlan 150 promiscuous ?
  <cr>

[Comware7-GigabitEthernet1/0/10]port private-vlan 150 promiscuous

[Comware7-GigabitEthernet1/0/10]interface g1/0/12

[Comware7-GigabitEthernet1/0/12]port access vlan 151

[Comware7-GigabitEthernet1/0/12]port private-vlan ?
  INTEGER<1-4094>  VLAN ID
  host             Specify the host mode in private VLAN

[Comware7-GigabitEthernet1/0/12]port private-vlan host

[Comware7-GigabitEthernet1/0/12]interface g1/0/14

[Comware7-GigabitEthernet1/0/14]port access vlan 152

[Comware7-GigabitEthernet1/0/14]port private-vlan host

[Comware7-GigabitEthernet1/0/14]quit


[Comware7]interface vlan 150

[Comware7-Vlan-interface150]ip address 10.150.2.1 24

[Comware7-Vlan-interface150]?
Vlan-interface interface view commands:
  arp                 ARP module
  bandwidth           Specify the expected bandwidth
  bfd                 BFD module
  cfd                 Connectivity Fault Detection (CFD) module
```

```
  ddns                  Dynamic Domain Name System (DDNS) module
  default               Restore the default settings
  description           Describe the interface
  dhcp                  Dynamic Host Configuration Protocol (DHCP) commands
  diagnostic-logfile    Diagnostic log file configuration
  display               Display current system information
  enable                Enable functions
  igmp                  Specify IGMP configuration information
  ip                    Specify IP configuration
  ipsec                 IP Security (IPsec) module
  ipv6                  Specify IPv6 configuration
  isis                  Configure interface parameters for IS-IS
  local-proxy-arp       Specify local proxy ARP function for same interface
  local-proxy-nd        Local ND proxy function
  logfile               Log file configuration
  mad                   Multi-active detection
  mld                   Specify MLD configuration information
  monitor               System monitor
  mpls                  Multiprotocol Label Switching (MPLS) module
  mtu                   Specify Maximum Transmission Unit(MTU) of the interface
  multicast             Multicast module
  ntp-service           Network Time Protocol (NTP) module
  ospf                  OSPF interface commands
  ospfv3                OSPFv3 interface commands
  packet-filter         Packet filter settings
  pim                   Protocol Independent Multicast (PIM) module
  ping                  Ping function
  portal                Portal authentication module
  private-vlan          Private VLAN function
  proxy-arp             Specify proxy ARP function
  proxy-nd              ND proxy function
  quit                  Exit from current command view
  return                Exit to User View
  rip                   Configure interface parameters for RIP
  ripng                 Configure interface parameters for RIPng
  rsvp                  Resource Reservation Protocol (RSVP) module
  save                  Save current configuration
  security-logfile      Security log file configuration
  service               Specify the service slot
  shutdown              Shut down the interface
  tcp                   Specify TCP parameters of the interface
  tracert               Tracert function
  udp-helper            UDP helper function
  undo                  Cancel current setting
  vrrp                  Virtual Router Redundancy Protocol(VRRP) module
  xconnect              Bind a VSI

[Comware7-Vlan-interface150]private-vlan ?
  secondary  Specify the secondary VLANs which can communicate at Layer 3

[Comware7-Vlan-interface150]private-vlan secondary ?
  INTEGER<1-4094>  Secondary VLAN ID

[Comware7-Vlan-interface150]private-vlan secondary 151 to 152 ?
  INTEGER<1-4094>  Secondary VLAN ID
  <cr>

[Comware7-Vlan-interface150]private-vlan secondary 151 to 152

[Comware7-Vlan-interface150]quit
```

```
[Comware7]display private-vlan
 Primary VLAN ID: 150
 Secondary VLAN ID: 151-152

 VLAN ID: 150
 VLAN type: Static
 Private VLAN type: Primary
 Route interface: Configured
 IPv4 address: 10.150.2.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0150
 Name: VLAN 0150
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/10         GigabitEthernet1/0/12
    GigabitEthernet1/0/13         GigabitEthernet1/0/14
    GigabitEthernet1/0/15

 VLAN ID: 151
 VLAN type: Static
 Private VLAN type: Isolated Secondary
 Route interface: Configured
 IPv4 address: 10.150.2.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0151
 Name: VLAN 0151
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/10         GigabitEthernet1/0/12
    GigabitEthernet1/0/13

 VLAN ID: 152
 VLAN type: Static
 Private VLAN type: Secondary
 Route interface: Configured
 IPv4 address: 10.150.2.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0152
 Name: VLAN 0152
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/10         GigabitEthernet1/0/14
    GigabitEthernet1/0/15
```

Cisco

```
Cisco(config)#vtp ?
  domain     Set the name of the VTP administrative domain.
  file       Configure IFS filesystem file where VTP configuration is stored.
  interface  Configure interface as the preferred source for the VTP IP updater
             address.
  mode       Configure VTP device mode
  password   Set the password for the VTP administrative domain
  pruning    Set the administrative domain to permit pruning
  version    Set the administrative domain to VTP version

Cisco(config)#vtp mode ?
  client       Set the device to client mode.
  off          Set the device to off mode.
  server       Set the device to server mode.
  transparent  Set the device to transparent mode.
```

```
Cisco(config)#vtp mode transparent ?
  mst      Set the mode for MST VTP instance.
  unknown  Set the mode for unknown VTP instances.
  vlan     Set the mode for VLAN VTP instance.
  <cr>

Cisco(config)#vtp mode transparent
Setting device to VTP Transparent mode for VLANS.


Cisco(config)#vlan 150
Cisco(config-vlan)#?
VLAN configuration commands:
  are           Maximum number of All Route Explorer hops for this VLAN (or
                zero if none specified)
  backupcrf     Backup CRF mode of the VLAN
  bridge        Bridging characteristics of the VLAN
  exit          Apply changes, bump revision number, and exit mode
  media         Media type of the VLAN
  mtu           VLAN Maximum Transmission Unit
  name          Ascii name of the VLAN
  no            Negate a command or set its defaults
  parent        ID number of the Parent VLAN of FDDI or Token Ring type VLANs
  private-vlan  Configure a private VLAN
  remote-span   Configure as Remote SPAN VLAN
  ring          Ring number of FDDI or Token Ring type VLANs
  said          IEEE 802.10 SAID
  shutdown      Shutdown VLAN switching
  state         Operational state of the VLAN
  ste           Maximum number of Spanning Tree Explorer hops for this VLAN (or
                zero if none specified)
  stp           Spanning tree characteristics of the VLAN
  tb-vlan1      ID number of the first translational VLAN for this VLAN (or
                zero if none)
  tb-vlan2      ID number of the second translational VLAN for this VLAN (or
                zero if none)

Cisco(config-vlan)#private-vlan ?
  association  Configure association between private VLANs
  community    Configure the VLAN as a community private VLAN
  isolated     Configure the VLAN as an isolated private VLAN
  primary      Configure the VLAN as a primary private VLAN

Cisco(config-vlan)#private-vlan primary ?
  <cr>

Cisco(config-vlan)#private-vlan primary

Cisco(config-vlan)#exit

Cisco(config)#vlan 151

Cisco(config-vlan)#private-vlan ?
  association  Configure association between private VLANs
  community    Configure the VLAN as a community private VLAN
  isolated     Configure the VLAN as an isolated private VLAN
  primary      Configure the VLAN as a primary private VLAN

Cisco(config-vlan)#private-vlan isolated ?
  <cr>

Cisco(config-vlan)#private-vlan isolated
```

```
Cisco(config-vlan)#exit

Cisco(config)#vlan 152

Cisco(config-vlan)#private-vlan ?
  association  Configure association between private VLANs
  community    Configure the VLAN as a community private VLAN
  isolated     Configure the VLAN as an isolated private VLAN
  primary      Configure the VLAN as a primary private VLAN

Cisco(config-vlan)#private-vlan community ?
  <cr>

Cisco(config-vlan)#private-vlan community

Cisco(config-vlan)#exit

Cisco(config)#vlan 150

Cisco(config-vlan)#private-vlan ?
  association  Configure association between private VLANs
  community    Configure the VLAN as a community private VLAN
  isolated     Configure the VLAN as an isolated private VLAN
  primary      Configure the VLAN as a primary private VLAN

Cisco(config-vlan)#private-vlan association ?
  WORD    VLAN IDs of the private VLANs to be configured
  add     Add a VLAN to private VLAN list
  remove  Remove a VLAN from private VLAN list

Cisco(config-vlan)#private-vlan association add ?
  WORD  VLAN IDs of the private VLANs to be configured

Cisco(config-vlan)#private-vlan association add 151-152 ?
  <cr>

Cisco(config-vlan)#private-vlan association add 151-152


Cisco(config)#interface g1/0/10

Cisco(config-if)#switchport ?
  access         Set access mode characteristics of the interface
  autostate      Include or exclude this port from vlan link up calculation
  backup         Set backup for the interface
  block          Disable forwarding of unknown uni/multi cast addresses
  host           Set port host
  mode           Set trunking mode of the interface
  nonegotiate    Device will not engage in negotiation protocol on this
                 interface
  port-security  Security related command
  priority       Set appliance 802.1p priority
  private-vlan   Set the private VLAN configuration
  protected      Configure an interface to be a protected port
  trunk          Set trunking characteristics of the interface
  voice          Voice appliance attributes
  <cr>

Cisco(config-if)#switchport mode ?
  access        Set trunking mode to ACCESS unconditionally
  dot1q-tunnel  set trunking mode to TUNNEL unconditionally
  dynamic       Set trunking mode to dynamically negotiate access or trunk mode
```

```
  private-vlan  Set private-vlan mode
  trunk         Set trunking mode to TRUNK unconditionally

Cisco(config-if)#switchport mode private-vlan ?
  host         Set the mode to private-vlan host
  promiscuous  Set the mode to private-vlan promiscuous

Cisco(config-if)#switchport mode private-vlan promiscuous ?
  <cr>

Cisco(config-if)#switchport mode private-vlan promiscuous

Cisco(config-if)#switchport private-vlan ?
  association       Set the private VLAN association
  host-association  Set the private VLAN host association
  mapping           Set the private VLAN promiscuous mapping

Cisco(config-if)#switchport private-vlan mapping ?
  <1006-4094>  Primary extended range VLAN ID of the private VLAN promiscuous
               port mapping
  <2-1001>     Primary normal range VLAN ID of the private VLAN promiscuous
               port mapping

Cisco(config-if)#switchport private-vlan mapping 150 ?
  WORD    Secondary VLAN IDs of the private VLAN promiscuous port mapping
  add     Add a VLAN to private VLAN list
  remove  Remove a VLAN from private VLAN list

Cisco(config-if)#switchport private-vlan mapping 150 add ?
  WORD  Secondary VLAN IDs of the private VLAN promiscuous port mapping

Cisco(config-if)#switchport private-vlan mapping 150 add 151-152 ?
  <cr>

Cisco(config-if)#switchport private-vlan mapping 150 add 151-152

Cisco(config)#interface g1/0/12

Cisco(config-if)#switchport mode private-vlan ?
  host         Set the mode to private-vlan host
  promiscuous  Set the mode to private-vlan promiscuous

Cisco(config-if)#switchport mode private-vlan host

Cisco(config-if)#switchport private-vlan ?
  association       Set the private VLAN association
  host-association  Set the private VLAN host association
  mapping           Set the private VLAN promiscuous mapping

Cisco(config-if)#switchport private-vlan host-association ?
  <1006-4094>  Primary extended range VLAN ID of the private VLAN host port
               association
  <2-1001>     Primary normal range VLAN ID of the private VLAN port
               association

Cisco(config-if)#switchport private-vlan host-association 150 ?
  <1006-4094>  Secondary extended range VLAN ID of the private VLAN host port
               association
  <2-1001>     Secondary normal range VLAN ID of the private VLAN host port
               association

Cisco(config-if)#switchport private-vlan host-association 150 151 ?
  <cr>
```

```
Cisco(config-if)#switchport private-vlan host-association 150 151

Cisco(config-if)#int g1/0/13

Cisco(config-if)#switchport mode private-vlan host

Cisco(config-if)#switchport private-vlan host-association 150 151

Cisco(config)#int g1/0/14

Cisco(config-if)#switchport mode private-vlan host

Cisco(config-if)#switchport private-vlan host-association 150 152

Cisco(config-if)#int g1/0/15

Cisco(config-if)#switchport mode private-vlan host

Cisco(config-if)#switchport private-vlan host-association 150 152

Cisco(config-if)#exit


Cisco(config)#interface vlan 150

Cisco(config-if)#ip addr 10.150.3.1 255.255.255.0

Cisco(config-if)#?
Interface configuration commands:
  aaa                     Authentication, Authorization and Accounting.
  access-expression       Build a bridge boolean access expression
  arp                     Set arp type (arpa, probe, snap) or timeout or log
                          options
  bandwidth               Set bandwidth informational parameter
  bgp-policy              Apply policy propagated by bgp community string
  bridge-group            Transparent bridging interface parameters
  carrier-delay           Specify delay for interface transitions
  cdp                     CDP interface subcommands
  clns                    CLNS interface subcommands
  crypto                  Encryption/Decryption commands
  cts                     Configure Cisco Trusted Security
  dampening               Enable event dampening
  datalink                Interface Datalink commands
  default                 Set a command to its defaults
  delay                   Specify interface throughput delay
  description             Interface specific description
  eou                     EAPoUDP Interface Configuration Commands
  exit                    Exit from interface configuration mode
  flow-sampler            Attach flow sampler to the interface
  glbp                    Gateway Load Balancing Protocol interface commands
  help                    Description of the interactive help system
  history                 Interface history histograms - 60 second, 60 minute
                          and 72 hour
  hold-queue              Set hold queue depth
  ip                      Interface Internet Protocol config commands
  ipv6                    IPv6 interface subcommands
  isis                    IS-IS commands
  iso-igrp                ISO-IGRP interface subcommands
  line-proto-delay        Enable line proto dealy interface
  link                    Configure Link
  load-interval           Specify interval for load calculation for an
                          interface
```

```
  logging                  Configure logging for interface
  loopback                 Configure internal loopback on an interface
  macro                    Command macro
  max-reserved-bandwidth   Maximum Reservable Bandwidth on an Interface
  mka                      MACsec Key Agreement (MKA) interface configuration
  neighbor                 interface neighbor configuration mode commands
  network-policy           Network Policy
  nmsp                     NMSP interface configuration
  no                       Negate a command or set its defaults
  ntp                      Configure NTP
  private-vlan             Configure private VLAN SVI interface settings
  rate-limit               Rate Limit
  routing                  Per-interface routing configuration
  service-policy           Configure CPL Service Policy
  shutdown                 Shutdown the selected interface
  snmp                     Modify SNMP interface parameters
  source                   Get config from another source
  spanning-tree            Spanning Tree Subsystem
  standby                  HSRP interface configuration commands
  timeout                  Define timeout values for this interface
  topology                 Configure routing topology on the interface
  traffic-shape            Enable Traffic Shaping on an Interface or
                           Sub-Interface
  vrf                      VPN Routing/Forwarding parameters on the interface
  vrrp                     VRRP Interface configuration commands
  vtp                      Enable VTP on this interface

Cisco(config-if)#private-vlan ?
  mapping  Set the private VLAN SVI interface mapping

Cisco(config-if)#private-vlan mapping ?
  WORD    Secondary VLAN IDs of the private VLAN SVI interface mapping
  add     Add a VLAN to private VLAN list
  remove  Remove a VLAN from private VLAN list

Cisco(config-if)#private-vlan mapping add ?
  WORD  Secondary VLAN IDs of the private VLAN SVI interface mapping

Cisco(config-if)#private-vlan mapping add 151-152 ?
  <cr>

Cisco(config-if)#private-vlan mapping add 151-152



Cisco#show vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
150     151       isolated          Gi1/0/10, Gi1/0/12, Gi1/0/13
150     152       community         Gi1/0/10, Gi1/0/14, Gi1/0/15

Cisco#show vlan private-vlan type

Vlan Type
---- -----------------
150  primary
151  isolated
152  community

Cisco#show interface private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
```

```
vlan150   151            isolated
vlan150   152            community
```

b) MVRP

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# mvrp enable	[Comware7]mvrp global enable	Cisco(config-if)#feature mvrp
ArubaOS-Switch(config)# interface 1 mvrp enable	[Comware7]interface g1/0/1	
	[Comware7-GigabitEthernet1/0/1]mvrp enable	
ArubaOS-Switch# show mvrp config	[Comware7]display mvrp running-status	
ArubaOS-Switch# show mvrp state 1	[Comware7]display mvrp state interface g1/0/1 vlan 1	
ArubaOS-Switch(config)# mvrp {enable | disable}		Cisco(config-if)#feature mvrp
ArubaOS-Switch(eth-1)#[no] mvrp join-timer <20-1000>		Cisco(config-if)#mvrp timer {join}
ArubaOS-Switch(eth-1)# [no] mvrp leave-timer <40-1000000>		Cisco(config-if)#mvrp timer {{join} timer-value | periodic}
ArubaOS-Switch(eth-1)# [no] mvrp leaveall-timer <500-1000000>		Cisco(config-if)#mvrp timer {| leave | join-leave}timer-value | periodic}
ArubaOS-Switch(eth-1)# [no] mvrp periodic-timer <100-1000000>		
ArubaOS-Switch(eth-1)#mvrp registration {normal |fixed		Cisco(config-if)#mvrp registration {normal | fixed |forbidden}
ArubaOS-Switch#show mvrp config		Cisco(config-if)#show mvrp interface
ArubaOS-Switch#show mvrp state <vlan-id> [<port-id>]		Cisco(config-if)#show mvrp interface type number
ArubaOS-Switch#show MVRP statistics [<PORT-LIST>]		Cisco(config-if)#show mvrp interface type number statistic
ArubaOS-Switch#show tech mvrp		Cisco(config-if)#show mvrp pruning interface type number
ArubaOS-Switch#clear mvrp statistics [<PORT-LIST>]		Cisco(config-if)#clear mvrp interface [interface type number]

ArubaOS-Switch

```
ArubaOS-Switch(config)# mvrp ?
```

```
 disable                Disable MVRP.
 enable                 Enable MVRP.

ArubaOS-Switch(config)# mvrp enable ?
 <cr>

ArubaOS-Switch(config)# mvrp enable

ArubaOS-Switch(config)# interface 1 ?
 arp-protect            Configure the port as trusted or untrusted.
 bandwidth-min          Configure guaranteed minimum bandwidth settings.
 broadcast-limit        Limit network bandwidth used by broadcast traffic.
 dhcp-snooping          Configure port-specific DHCP snooping parameters.
 dhcpv6-snooping        Configure DHCPv6 snooping on the port.
 disable                Disable the port.
 dldp                   Enable or disable the Device Link Detection Protocol (DLDP) to
                        monitor link status.
 enable                 Enable the port.
 energy-efficient-e... Enable energy-efficient-ethernet on the port.
 flow-control           Enable flow control negotiation on the port during link
                        establishment.
 forbid                 Prevent this port from becoming a member of the specified
                        VLAN(s).
 gvrp                   Set the GVRP timers for the port.
 ignore-untagged-mac
 ip                     Apply the specified IPv4 ACL to inbound or outbound packets on
                        this interface.
 ipv6                   Configure various IPv6 parameters for the VLAN.
 lacp                   Define whether LACP is enabled on the port, and whether it is in
                        active or passive mode when enabled.
 link-keepalive         Configure UniDirectional Link Detection (UDLD) on the port.
 mac-count-notify       Send a trap when the number of MAC addresses learned on the
                        specified ports exceeds the threshold.
 mac-notify             Configure SNMP traps for changes in the MAC address table.
 mdix-mode              Set port MDI/MDIX mode (default: auto).
 monitor                Monitor traffic on the port.
 mvrp                   Configure the Multiple VLAN Registration Protocol (MVRP).
 name                   Assign an interface name.
 poe-allocate-by        Configure the power allocation method.
 poe-lldp-detect        Allow the link partner to specify power allocation using LLDP.
 poe-value              Set the maximum power allocation for the port.
 power-over-ethernet    Enable per-port power distribution.
 private-vlan           Configure ports as promiscuous members of private VLANs.
 qos                    Configure port-based traffic prioritization.
 rate-limit             Enable rate limiting for various types of traffic.
 service-policy         Apply a service-policy on the interface.
 smart-link             Configure the control VLANs for receiving flush packets.
 speed-duplex           Define mode of operation for the port(s).
 tagged                 Configure this port as a tagged member of the specified VLAN(s).
 unknown-vlans          Configure the GVRP mode.
 untagged               Configure this port as an untagged member of the specified VLAN.
 <cr>

ArubaOS-Switch(config)# interface 1 mvrp ?
 disable                Disable MVRP.
 enable                 Enable MVRP.
 join-timer             Set the join timer for the port.
 leave-timer            Set the leave timer for the port.
 leaveall-timer         Set the leaveall timer for the port.
 periodic-timer         Set the periodic timer transmission interval for the port.
 periodic-timer-enable Enable periodic timer transmission for the port.
 registration           Configure how the port responds to MRP messages.
```

```
ArubaOS-Switch(config)# interface 1 mvrp enable ?
 <cr>

ArubaOS-Switch(config)# interface 1 mvrp enable



ArubaOS-Switch# show mvrp ?
 config                Show the MVRP configuration for all ports.
 state                 Show the MVRP state.
 statistics            Show MVRP statistics.

ArubaOS-Switch# show mvrp config ?
 <cr>

ArubaOS-Switch# show mvrp config

 Configuration and Status - MVRP

 Global MVRP status : Enabled

 Port     Status   Periodic Registration Join  Leave    LeaveAll Periodic
                   Timer    Type         Time  Timer    Timer    Timer
 -------  -------- -------- ------------ ----  -------- -------- --------
 1        Enabled  Enabled  Normal       20    300      1000     100
 2        Disabled Enabled  Normal       20    300      1000     100
 3        Disabled Enabled  Normal       20    300      1000     100
 4        Disabled Enabled  Normal       20    300      1000     100
 5        Disabled Enabled  Normal       20    300      1000     100
 6        Disabled Enabled  Normal       20    300      1000     100
(output omitted)

ArubaOS-Switch# show mvrp state ?
 VLAN-ID               Enter a VLAN identifier or the VLAN name if configured.

ArubaOS-Switch# show mvrp state 1 ?
 [ethernet] PORT-NUM
 <cr>

ArubaOS-Switch# show mvrp state 1

 Configuration and Status - MVRP state for VLAN 1

 Port     VLAN  Registrar Applicant Forbid
               State     State     Mode
 -------- ----- --------- --------- ---------
 1        1     MT        QA        No
```

Comware5

```
[Comware5]mvrp ?
  global           Specify the global configuration
  gvrp-compliance  Specify the GVRP-compliant mode

[Comware5]mvrp global ?
  enable  Enable MVRP

[Comware5]mvrp global enable ?
  <cr>

[Comware5]mvrp global enable
```

```
[Comware5]interface g1/0/1

[Comware5-GigabitEthernet1/0/1]?
Gigabitethernet_l2 interface view commands:
  apply                   Apply Poe-profile
  arp                     Configure ARP for the interface
  bpdu-drop               Drop BPDU packets.
  bpdu-tunnel             Specify BPDU tunnel function
  broadcast-suppression   Specify the broadcast storm control
  cfd                     Connectivity fault detection (IEEE 802.1ag)
  default                 Restore the default settings
  description             Describe the interface
  dhcp-snooping           DHCP Snooping
  display                 Display current system information
  dldp                    Specify configuration information of DLDP
  dot1x                   Specify 802.1X configuration information
  duplex                  Status of duplex
  enable                  Enable function
  flow-control            Flow control command
  flow-interval           Set interval of interface statistic
  garp                    Generic Attribute Registration Protocol
  gvrp                    GARP VLAN Registration Protocol
  igmp-snooping           Configure IGMP snooping characteristic
  ip                      Specify IP configurations for the system
  ipv6                    IPv6 status and configuration information
  jumboframe              Jumboframe command
  lacp                    Configure LACP Protocol
  link-aggregation        Link aggregation group
  link-delay              Set the delay time of holding link-up and link-down
  lldp                    Link Layer Discovery Protocol(802.1ab)
  loopback                Specify loopback of current port
  loopback-detection      Detect if loopback exists
  mac-address             Configure MAC address
  mac-authentication      MAC authentication configuration
  mac-forced-forwarding   Specify MAC-forced forwarding configuration
                          information
  mac-vlan                Specify MAC VLAN
  mdi                     Specify mdi type
  mirroring-group         Specify mirroring-group
  mirroring-port          Specify mirroring port
  mld-snooping            Configure MLD snooping characteristic
  monitor-port            Specify monitor port
  mrp                     Multiple Register Protocol
  mtracert                Trace route to multicast source
  multicast-suppression   Specify the multicast storm control
  mvrp                    Multiple VLAN Registration Protocol
  ndp                     Neighbor discovery protocol
  ntdp                    Specify NTDP configuration information
  oam                     OAM protocol
  packet-filter           Specify packet filter
  ping                    Ping function
  poe                     Configure PoE port
  port                    Configure or modify aggregate parameters on a port
  port-isolate            Specify port-isolate configuration information
  port-security           Specify port-security configuration information
  portal                  Portal protocol
  qinq                    Specify 802.1Q-in-Q VPN function
  qos                     Command of QoS(Quality of Service)
  quit                    Exit from current command view
  return                  Exit to User View
  rmon                    Specify RMON
  save                    Save current configuration
```

```
  sflow                   Specify sFlow configuration information
  shutdown                Shut down this interface
  smart-link              Configure smart link
  speed                   Specify speed of current port
  storm-constrain         Port storm-constrain
  stp                     Spanning tree protocol
  tracert                 Trace route function
  undo                    Cancel current setting
  unicast-suppression     Specify the unicast storm control
  virtual-cable-test      Virtual cable test information
  vlan                    Set VLAN precedence
  voice                   Specify voice VLAN

[Comware5-GigabitEthernet1/0/1]mvrp ?
  enable        Enable MVRP on port
  registration  MVRP registration mode

[Comware5-GigabitEthernet1/0/1]mvrp enable ?
  <cr>

[Comware5-GigabitEthernet1/0/1]mvrp enable

[Comware5-GigabitEthernet1/0/1]quit



[Comware5]display mvrp ?
  running-status  MVRP running status
  state           MVRP machine information
  statistics      MVRP packet statistics
  vlan-operation  Dynamic VLAN operation information

[Comware5]display mvrp running-status ?
  interface  Specify the interface
  |          Matching output
  <cr>

[Comware5]display mvrp running-status
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

[Comware5]display mvrp state ?
  interface  Specify the interface

[Comware5]display mvrp state interface g1/0/1 ?
  vlan  Specify the VLAN ID

[Comware5]display mvrp state interface g1/0/1 vlan ?
  INTEGER<1-4094>  VLAN ID

[Comware5]display mvrp state interface g1/0/1 vlan 1 ?
  |     Matching output
  <cr>

[Comware5]display mvrp state interface g1/0/1 vlan 1
```

Comware7

```
[Comware7]mvrp ?
  global           Specify global configuration
  gvrp-compliance  Specify GVRP-compliance configuration
```

```
[Comware7]mvrp global ?
  enable  Enable multiple VLAN registration protocol

[Comware7]mvrp global enable ?
  <cr>
[Comware7]mvrp global enable

[Comware7]interface g1/0/1

[Comware7-GigabitEthernet1/0/1]?
Gigabitethernet_l2 interface view commands:
  apply                   Apply a PoE profile
  arp                     ARP module
  bandwidth               Specify the expected bandwidth
  bpdu-drop               Specify BPDU drop function
  broadcast-suppression   Broadcast storm suppression function
  cdp                     Non standard IEEE discovery protocol
  cfd                     Connectivity Fault Detection (CFD) module
  dcbx                    Data Center Bridge Capability Exchange Protocol
  default                 Restore the default settings
  description             Describe the interface
  dhcp                    DHCP module
  diagnostic-logfile      Diagnostic log file configuration
  display                 Display current system information
  dldp                    DLDP module
  dot1x                   802.1X module
  duplex                  Status of duplex
  eee                     Energy efficient ethernet
  enable                  Enable functions
  evb                     Edge Virtual Bridging (EVB) module
  flex10                  Configure Flex10
  flow-control            Enable flow control function
  flow-interval           Set the interface statistics interval
  igmp-snooping           IGMP snooping module
  ip                      Specify IP configuration
  ipv6                    Specify IPv6 configuration
  jumboframe              Specify jumbo frame forwarding
  l2vpn                   Layer 2 Virtual Private Network (L2VPN) module
  lacp                    Configure LACP protocol
  link-aggregation        Specify link aggregation group configuration
                          information
  link-delay              Set the physical state change suppression
  lldp                    Link Layer Discovery Protocol(802.1ab)
  logfile                 Log file configuration
  loopback                Specify loopback of current port
  loopback-detection      Loopback detection module
  mac-address             Configure MAC address
  mac-authentication      MAC authentication module
  mac-forced-forwarding   Specify MAC-forced forwarding configuration information
  mac-vlan                MAC VLAN configuration
  macsec                  MAC security module
  mdix-mode               Specify mdix type
  mirroring-group         Specify mirroring group
  mka                     MACsec Key Agreement protocol
  mld-snooping            MLD snooping module
  monitor                 System monitor
  mrp                     Multiple registration protocol
  multicast-suppression   Multicast storm suppression function
  mvrp                    Multiple VLAN registration protocol
  oam                     OAM module
  packet-filter           Packet filter settings
  pbb                     Provider Backbone Bridge (PBB) module
```

```
  ping                    Ping function
  poe                     Power over Ethernet
  port                    Set port attributes
  port-isolate            Port isolation configuration
  port-security           Port security module
  priority-flow-control   Priority-based flow control (PFC) configuration
  ptp                     Precision Time Protocol (PTP) module
  qcn                     Quantized Congestion Notification (QCN) module
  qinq                    802.1QinQ function
  qos                     Quality of Service (QoS) module
  quit                    Exit from current command view
  return                  Exit to User View
  rmon                    RMON module
  save                    Save current configuration
  security-logfile        Security log file configuration
  service-instance        Configure a service instance
  sflow                   sFlow function
  shutdown                Shut down the interface
  smart-link              Smart Link module
  spbm                    SPBM configuration
  speed                   Specify speed of current port
  storm-constrain         Port storm control
  stp                     Spanning Tree Protocol (STP) module
  tracert                 Tracert function
  trill                   TRansparent Interconnection of Lots of Links (TRILL)
                          module
  undo                    Cancel current setting
  unicast-suppression     Unicast storm suppression function
  virtual-cable-test      Test cable connection for an interface
  vlan                    Set VLAN precedence
  voice-vlan              Voice VLAN configuration

[Comware7-GigabitEthernet1/0/1]mvrp ?
  enable        Enable multiple VLAN registration protocol
  registration  Specify MVRP registration mode

[Comware7-GigabitEthernet1/0/1]mvrp enable ?
  <cr>

[Comware7-GigabitEthernet1/0/1]mvrp enable



[Comware7]display mvrp ?
  running-status  Display MVRP running status
  state           Display MVRP state of a port
  statistics      Display MVRP statistics

[Comware7]display mvrp running-status ?
  >          Redirect it to a file
  >>         Redirect it to a file in append mode
  interface  Interface configuration
  |          Matching output
  <cr>

[Comware7]display mvrp running-status
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1]----
 Config Status                  : Enabled
 Running Status                 : Disabled
```

```
 Join Timer                      : 20 (centiseconds)
 Leave Timer                     : 60 (centiseconds)
 Periodic Timer                  : 100 (centiseconds)
 LeaveAll Timer                  : 1000 (centiseconds)
 Registration Type               : Normal
 Registered VLANs :
  None
 Declared VLANs :
  None
 Propagated VLANs :
  None

[Comware7]display mvrp state ?
  interface  Interface configuration

[Comware7]display mvrp state interface g1/0/1 ?
  vlan  VLAN configuration

[Comware7]display mvrp state interface g1/0/1 vlan ?
  INTEGER<1-4094>  VLAN ID

[Comware7]display mvrp state interface g1/0/1 vlan 1 ?
  >     Redirect it to a file
  >>    Redirect it to a file in append mode
  |     Matching output
  <cr>

[Comware7]display mvrp state interface g1/0/1 vlan 1
 MVRP state of VLAN 1 on port GE1/0/1
 Port                      VLAN   App-state   Reg-state
 ------------------------ ------ ----------- -----------
 GE1/0/1                      1       VO          MT
```

c) VxLAN

ArubaOS-Switch	Comware7	Cisco
(example config for HPE 3810)	(example config for HPE 5930)	(example config for Nexus 9000)
ArubaOS-Switch(config)# vxlan enable	[Comware7] l2vpn enable	Cisco-vtep-1(config)# feature pim
ArubaOS-Switch(config)# vxlan udp 12345	[Comware7] vsi vpna	Cisco-vtep-1(config)# ip pim rp-address 10.0.111.22 group-list 224.0.0.0/4
ArubaOS-Switch(config)# interface tunnel 1	[Comware7-vsi-vpna] vxlan 200	Cisco-vtep-1(config)# interface loopback0
ArubaOS-Switch(tunnel-1)# tunnel mode vxlan	[Comware7-vsi-vpna-vxlan200] quit [Comware7-vsi-vpna] quit	Cisco-vtep-1(config-if)# ip pim sparse-mode
ArubaOS-Switch(tunnel-1)# tunnel source 10.222.1.2	[Comware7] interface tunnel 1 mode vxlan	Cisco-vtep-1(config-if)# exit
ArubaOS-Switch(tunnel-1)# tunnel destination 10.222.1.1	[Comware7-Tunnel1] source 10.222.2.2	Cisco-vtep-1(config)# interface e2/1
ArubaOS-Switch(tunnel-1)# exit	[Comware7-Tunnel1] destination 10.222.2.1	Cisco-vtep-1(config-if)# ip pim sparse-mode
ArubaOS-Switch(config)# virtual-network 1 10 virtual-net1	[Comware7-Tunnel1] quit	Cisco-vtep-1(config-if)# exit
ArubaOS-Switch(config)# vxlan tunnel 1 overlay-vlan 10	[Comware7] vsi vpna	Cisco-vtep-1(config)# feature nv overlay

	[Comware7-vsi-vpna] vxlan 200	Cisco-vtep-1(config)# feature vn-segment-vlan-based
	[Comware7-vsi-vpna-vxlan200] tunnel 1	Cisco-vtep-1(config)# interface nve1
	[Comware7-vsi-vpna-vxlan200] quit [Comware7-vsi-vpna] quit	Cisco-vtep-1(config-if)# no shutdown
	[Comware7] interface g1/0/1	Cisco-vtep-1(config-if)# source-interface loopback0
	[Comware7-GigabitEthernet1/0/1] service-instance 1000	Cisco-vtep-1(config-if)# member vni 10000 mcast-group 230.1.1.1
	[Comware7-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 2	Cisco-vtep-1(config-if)# exit
	[Comware7-GigabitEthernet1/0/1-srv1000] xconnect vsi vpna	Cisco-vtep-1(config)# vlan 200
	[Comware7-GigabitEthernet1/0/1-srv1000] quit [Comware7-GigabitEthernet1/0/1] quit	Cisco-vtep-1(config-vlan)# vn-segment 10000
		Cisco-vtep-1(config-vlan)# exit Cisco-vtep-1(config)# exit

ArubaOS-Switch

```
(example config for HPE 3810)

ArubaOS-Switch(config)# vxlan enable

ArubaOS-Switch(config)# vxlan udp 12345

ArubaOS-Switch(config)# interface tunnel 1

ArubaOS-Switch(tunnel-1)# tunnel mode vxlan

ArubaOS-Switch(tunnel-1)# tunnel source 10.222.1.2

ArubaOS-Switch(tunnel-1)# tunnel destination 10.222.1.1

ArubaOS-Switch(config)# virtual-network 1 10 virtual-net1

ArubaOS-Switch(config)# vxlan tunnel 1 overlay-vlan 10
```

Comware5

```
(not an available feature)
```

Comware7

```
(example config for HPE 5930)

[Comware7] l2vpn enable

[Comware7] vsi vpna

[Comware7-vsi-vpna] vxlan 200
```

```
[Comware7-vsi-vpna-vxlan200] quit

[Comware7-vsi-vpna] quit

[Comware7] interface tunnel 1 mode vxlan

[Comware7-Tunnel1] source 10.222.2.2

[Comware7-Tunnel1] destination 10.222.2.1

[Comware7-Tunnel1] quit

[Comware7] vsi vpna

[Comware7-vsi-vpna] vxlan 200

[Comware7-vsi-vpna-vxlan200] tunnel 1

[Comware7-vsi-vpna-vxlan200] quit

[Comware7-vsi-vpna] quit

[Comware7] interface g1/0/1

[Comware7-GigabitEthernet1/0/1] service-instance 1000

[Comware7-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 2

[Comware7-GigabitEthernet1/0/1-srv1000] xconnect vsi vpna

[Comware7-GigabitEthernet1/0/1-srv1000] quit

[Comware7-GigabitEthernet1/0/1] quit
```

Cisco

```
(example config for Nexus 9000)

Cisco-vtep-1(config)# feature pim

Cisco-vtep-1(config)# ip pim rp-address 10.0.111.22 group-list 224.0.0.0/4

Cisco-vtep-1(config)# interface loopback0

Cisco-vtep-1(config-if)# ip pim sparse-mode

Cisco-vtep-1(config-if)# exit

Cisco-vtep-1(config)# interface e2/1

Cisco-vtep-1(config-if)# ip pim sparse-mode

Cisco-vtep-1(config-if)# exit

Cisco-vtep-1(config)# feature nv overlay

Cisco-vtep-1(config)# feature vn-segment-vlan-based

Cisco-vtep-1(config)# interface nve1

Cisco-vtep-1(config-if)# no shutdown

Cisco-vtep-1(config-if)# source-interface loopback0
```

```
Cisco-vtep-1(config-if)# member vni 10000 mcast-group 230.1.1.1

Cisco-vtep-1(config-if)# exit

Cisco-vtep-1(config)# vlan 200

Cisco-vtep-1(config-vlan)# vn-segment 10000

Cisco-vtep-1(config-vlan)# exit

Cisco-vtep-1(config)# exit
```

d) MDNS, IPv6 ND snooping, BFD

ArubaOS-Switch	Cisco
ArubaOS-Switch(config)#mdns default	Cisco(config)#service-routing mdns-sd
ArubaOS-Switch(config)#show mdns	Cisco(config)#show mdns statistics all
ArubaOS-Switch(config)#preview-mode	
(prev-mode)ArubaOS-Switch(config)# fabric-offload multicast ipv4 route enable	Cisco(config-if)#switchport mode fex-fabric
ArubaOS-Switch (config)# ipv6 nd snooping mac-check	Cisco(config)#ipv6 neighbor binding vlan vlan-id {interface type number | ipv6-address | mac-address}[tracking [disable | enable |retry-interval value] | reachable-lifetime value]
ArubaOS-Switch(config)#[no] ipv6 nd snooping	Cisco(config)#ipv6 snooping policy snooping-policy
ArubaOS-Switch(config)#[no] ipv6 nd snooping vlan [VLAN-ID-RANGE]	Cisco(config)#ipv6 nd inspection attach-policy [policy policy-name] | vlan {add | except | none | remove | all} vlan [vlan1, vlan2,vlan3...]]
ArubaOS-Switch(config)#clear ipv6 nd snooping [ipv6-address | vlan <vlan-id> | mac <mac-addr>]	Cisco(config-nd-inspection)#drop-unsecure
ArubaOS-Switch(interface)#[no] ipv6 nd snooping max-binding <value>	Cisco(config-nd-inspection)#ipv6 neighbour binding logging
ArubaOS-Switch(config)#[no] ipv6 nd snooping max-binding <port-list> <value>	Cisco(config)# ipv6 neighbor binding max-entries entries [vlan-limit number | interface-limit number | mac-limit number]
ArubaOS-Switch(interface)# ipv6 nd snooping trust	Cisco(config-nd-inspection)#trusted port
ArubaOS-Switch(config)#snmp-server enable traps nd-snooping [out-of-resources | violations]	Cisco(config-nd-inspection)# ipv6 destination-guard attach-policy policy-name
ArubaOS-Switch(vlan)# no ipv6 nd snooping prefix-list [IPV6-ADDR]	Cisco(config)#ipv6 snooping policy <snnoping-policy-id>
ArubaOS-Switch#show ipv6 nd snooping	Cisco(config-nd-inspection)#show ipv6 snooping capture-policy [interface type number
ArubaOS-Switch#show ipv6 nd snooping bindings	Cisco(config-nd-inspection)#show ipv6 snooping counter [interface type number]

ArubaOS-Switch#show ipv6 nd snooping statistics	Cisco(config-nd-inspection)#show ipv6 snooping counter [interface type number
ArubaOS-Switch(config)#bfd {enable | disable}	Cisco(config)#feature bfd
ArubaOS-Switch(config)#bfd echo-src-ip-address 23.2.2.2	Cisco(config-vlanbfd interval milliseconds min_rx milli seconds multiplier interval-multiplier
ArubaOS-Switch(config)#vlan 20 ip ospf 20.1.1.2 bfd	
ArubaOS-Switch(config)#vlan 21 vrrp vrid 1 bfd 21.1.1.2	
ArubaOS-Switch(config)#vlan 20 bfd min-transmit-interval 20 min-receive-interval 4 detect-multiplier 3	Cisco(config-vlan)#interval min-tx milliseconds min-rx milliseconds multiplier multiplier-value
ArubaOS-Switch(config)#[no] vlan 20 bfd min-echo-receive-interval 1000	Cisco(config-vlan)#bfd slow-timer milliseconds
ArubaOS-Switch(config)#vlan 20 bfd authentication keyed-sha1 0 key simple password	Cisco(config-vlan)#xconnect peer-ip-address vc-id {encapsulation mpls [manual] | pw-class pw-class-name} [pw-class pw-class-name] [sequencing {transmit | receive | both}
ArubaOS-Switch(config)#vlan 20 bfd authentication encrypted-password zVsjSMoTApAomza536tyHBw1mT9drR8nUFijdeMVtFg=	
ArubaOS-Switch(config)#[no] vlan 20 bfd authentication	
ArubaOS-Switch(config)#show bfd-session	Cisco(config)#show ip static route bfd
ArubaOS-Switch(config)#show bfd-session <session-no>	Cisco(config)#show bfd neighbours [detail]

e) RIPNG

ArubaOS-Switch	Cisco
ArubaOS-Switch(config)#router ripng	Cisco(config)#ipv6 unicast-routing
ArubaOS-Switch(config)#router ripng default-metric <1-15>	Cisco(config)#ipv6 rip name default-information {only | originate} [metric metric-value value
ArubaOS-Switch(config)#router ripng distance <1-255>	Cisco(config)#vrf definition vrf-name
ArubaOS-Switch(config)#router ripng redistribute	Cisco(config)#redistribute protocol [process-id] {level-1 | level-1-2| level-2} [metric metric-value] [metric-type{internal | external}] [route-map map-name]

ArubaOS-Switch(config)#router ripng timers	Cisco(config)#timers (IPv6 RIP)
ArubaOS-Switch(config)#router ripng trap	
ArubaOS-Switch(config)#vlan <VLAN-ID> ipv6 ripng enable	Cisco(config)#ipv6 rip vrf-mode enable
ArubaOS-Switch(config)#vlan <VLAN-ID> ipv6 ripng metric <1-15>	Cisco(config)#ipv6 router rip rip-process-name
ArubaOS-Switch(config)#show ipv6 ripng general	Cisco(config)#show ipv6 route
ArubaOS-Switch(config)#show ipv6 ripng peer	Cisco(config)#show ipv6 rip [name][database| next-hops]
ArubaOS-Switch(config)#show ipv6 ripng interface	Cisco(config)#show ipv6 route [ipv6-address| ipv6-prefix/prefix-length| protocol | interface-type interface-number]
ArubaOS-Switch(config)#show ipv6 ripng interface vlan <VLAN-ID>	Cisco(config)#show ipv6 route rip
ArubaOS-Switch(config)#show ipv6 ripng redistribute	Cisco(config)#show ipv6 rip vrf vrf-name next-hops
ArubaOS-Switch(config)#show ipv6 ripng traps	Cisco(config)#show ipv6 rip vrf vrf-name dataase
ArubaOS-Switch(config)#show ipv6 route ripng	
ArubaOS-Switch(config)#show ipv6 route ripng <IPv6-Address>	
ArubaOS-Switch(config)#router ospf3 redistribute ripng	Cisco(config)#route-map map-tag [permit | deny] [sequence-number]

f) IP-SLA, Portscan detection

ArubaOS-Switch	Cisco
ArubaOS-Switch(config)#ip-sla <ID> schedule { {now | startTime <START-TIME>} { { forever | stopTime <STOP-TIME> } [repetitions <NUM>] [frequency <FREQUENCY>]	Cisco(config)#ip sla endpoint-list type ip test
ArubaOS-Switch(config)#ip-sla <ID> history-size <SIZE>	Cisco(config)#ip-sla operation number
ArubaOS-Switch(config)#ip-sla <ID> tos <VALUE>	Cisco(config)#history buckets-kept size
ArubaOS-Switch(config)#ip-sla <ID> monitor threshold-config { rtt | srcTodstTime | dstToSrcTime} threshold-type { immediate | consecutive <count> } threshold-	Cisco(config)# ip sla monitor group schedule group-operation-number operation-id-numbers schedule-period seconds [ageout seconds] [frequency [seconds | range random-frequency-range]] [life { forever | seconds }] [start-time { hh : mm [: ss] [month day | day month] | pending | now | after

value <upper-limit> <lower-limit> action-type {trap | log | trap-log | none }	hh : mm : ss }]
ArubaOS-Switch(config)#ip-sla <ID> monitor packet-loss threshold-type { immediate | consecutive <count> } action-type {trap | log | trap-log | none }	Cisco(config)#ip sla schedule operation-number [life {forever | seconds}] [start-time {[hh:mm:ss] [month day | day month] | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]
ArubaOS-Switch(config)#ip-sla <ID> monitor test-completion action-type {trap | log | trap-log | none }	Cisco(config)#ip sla monitor
ArubaOS-Switch(config)#ip-sla <ID> icmp-echo {<DEST-IP> | Hostname} {source <IP> | source-interface {VLAN}}	Cisco(config)# icmp-echo {destination-ip-address | destination-hostname} [source-ip {ip-address | hostname} | source-interface interface-name]
ArubaOS-Switch(config)#ip-sla <ID> udp-echo {destination {<IP-ADDR>|<HOSTNAME>} <PORT-NUM>} {source <IP-ADDR>|<VLAN- ID>}[payload-size <SIZE>]	Cisco(config)#rtr responder type udpEcho
ArubaOS-Switch(config)#ip-sla <ID> tcp-connect {destination {<IP-ADDR>|<HOSTNAME>} <PORT-NUM>} {source {<IP-ADDR>|<VLAN>} <PORT-NUM>}	Cisco(config)#rtr responder type tcpConnect
ArubaOS-Switch(config)#ip-sla responder <sla-type> <IP-ADDR> <PORT-NUM>	Cisco(config)#rtr responder type tcpConnect ipaddress <ip-address> port <port>
ArubaOS-Switch(config)#show ip-sla <ID>	Cisco(config)#show rtr configuration
ArubaOS-Switch(config)#show ip-sla <ID> message-statistics	Cisco(config)#show ip sla mpls-lsp-monitor scan-queue
ArubaOS-Switch(config)#show ip-sla <ID> history	Cisco(config)#show ip sla auto group
ArubaOS-Switch(config)#show ip-sla responder	Cisco(config)#show ip sla auto template
ArubaOS-Switch(config)#show ip-sla responder message-statistics	Cisco(config)#show ip sla auto template type ip icmp-echo
ArubaOS-Switch(config)#show ip-sla 1	Cisco(config)#show ip sla monitor configuration
ArubaOS-Switch(config)#show ip-sla responder	Cisco(config)#show ip sla reaction-configuation
ArubaOS-Switch(config)#ip-sla <ID> dhcp source <VLAN-ID>	
ArubaOS-Switch(config)#ip-sla <ID> dns target-hostname <HOSTNAME> name-server <IP-ADDR>	Cisco(config)#dns{destination-ip-address|destination-hostname}name-serverip-address[source-ip{ip-address|hostname}source-portport-number]
ArubaOS-Switch(config)#ip-sla <ID> udp-jitter destination {<IP-ADDR>|<HOSTNAME>}	Cisco(config)#config- ip-sla-multicast-jitter-oper

<PORT-NUM> source {<IP-ADDR>|<VLAN-ID>} <PORT-NUM> [payload-size <SIZE>] [num-of-packets <NUM>] [packet-interval <INT>]	
ArubaOS-Switch(config)#ip-sla <ID> type udp-jitter-voip destination {<IP-ADDR> | <HOSTNAME>}<PORT-NUM> source {<IP-ADDR> | <VLAN-ID>} <PORT-NUM> [codec-type <CODEC-TYPE>] [advantage-factor <VALUE>]	Cisco(config)#config-ip-sla-voip
ArubaOS-Switch(config)#ip-sla responder <SLA-TYPE> <IP-ADDR> <PORT-NUM> source <IP-ADDR>	Cisco(config)#ip sla monitor responder
ArubaOS-Switch(config)#ip-sla <ID> monitor threshold-config { sd-jitter-pos|ds-jitter-pos|rtt|srcTodstTime|dstToSrcTime|mos|icpif} threshold-type { immediate | aggregated | consecutive <count> } threshold-value <upper-limit> <lower-limit> action-type {trap | log | trap-log | none }	Cisco(config)#ip sla reaction-configuration operation-number[react monitored-element[action-typeoption][threshold-type{average[number-of-measurements]| consecutive[occurrences]| immediate|never|xofy[x-valuey-value]}] [threshold-valueupper-thresholdlower-threshold]]
ArubaOS-Switch(config)#Show ip-sla <ID> results	Cisco(config)#show ip sla configuration
ArubaOS-Switch(config)#show ip-sla <ID> aggregated-results	Cisco(config)#show ip sla statistics aggregated and show ip sla statistics aggregated details
ArubaOS-Switch(config)#sh ip-sla responder <SLA-TYPE> statistics <IP-ADDR> <PORT-NUM> source <IP-ADDR>	Cisco(config)#sh ip sla responder
ArubaOS-Switch(config)#clear ip-sla responder <SLA-TYPE> statistics <IP-ADDR> <PORT-NUM> source <IP-ADDR>	
ArubaOS-Switch(config)#portscan-detection help	Cisco(config)#threat-detection help
ArubaOS-Switch(config)#portscan-detection	Cisco(config)#threat-detection scanning-threat shun duration 10
ArubaOS-Switch(config)#show portscan-detection	Cisco(config)# threat-detection statistics
ArubaOS-Switch(config)#show portscan-detection triggered-hosts	Cisco(config)# threat-detection statistics host [number-of-rate {1 |2 | 3}]
ArubaOS-Switch(config)#show portscan-detection ignored-hosts help ArubaOS-Switch(config)#show portscan-detection ignored-hosts	Cisco(config)#show threat-detection statistics [min-display-rate min_display_rate] top [[access-list | host | port-protocol] [rate-1 | rate-2 | rate-3] | tcp-intercept [all] detail]]

ArubaOS-Switch(config)#show portscan-detection port-statistics	Cisco(config)# threat-detection statistics

ArubaOS-Switch

```
ArubaOS-Switch(config)# ip-sla <ID> monitor <TAB>

 threshold-config     Set upper and lower threshold parameters

  packetLoss          Configure threshold-action values when packet loss happens

testCompletion        Configure action to be taken when test gets completed


ArubaOS-Switch(config)# ip-sla <ID> monitor threshold-config <TAB>

     rtt               Configure threshold-action values for RTT

srcTodstTime           Configure threshold-action values for src-to-dst (oneway) time

dstToSrcTime           Configure threshold-action values for dst-to-src (oneway) time


ArubaOS-Switch(config)# ip-sla <ID> monitor threshold-config RTT <TAB>

threshold-value        Configure threshold-value to trigger action

threshold-type         Configure threshold-type to decide when to trigger


ArubaOS-Switch(config)# ip-sla <ID> monitor threshold-config RTT threshold-type <TAB>

    immediate            Trigger action immediately when the threshold is hit

   consecutive         Trigger action after threshold is hit consecutively for configured
                                    number of times


ArubaOS-Switch(config)# ip-sla <ID> monitor threshold-config RTT threshold-type consecutive
<TAB>

     count          Configure Number of times threshold to be hit before triggering action


ArubaOS-Switch(config)# ip-sla <ID> monitor threshold-config RTT threshold-type
consecutive 5 <TAB>

threshold-value     Configure threshold values


ArubaOS-Switch(config)# ip-sla <ID> monitor threshold-config RTT threshold-type
consecutive 5 threshold-value <TAB>

upper-limit   Configure upper threshold limit
```

```
ArubaOS-Switch(config)# ip-sla <ID> monitor threshold-config RTT threshold-type
consecutive 5 threshold-value 50 <TAB>

lower-limit          Configure lower threshold limit

ArubaOS-Switch(config)# ip-sla <ID> history-size <TAB>

<SIZE>               Number of history records to be stored for the IP SLA.



ArubaOS-Switch(config)# ip-sla <ID> tos <TAB>

<TOS-VALUE>          Specify TOS Value to be set for the IP SLA test packet (0-255).



ArubaOS-Switch(config)# ip-sla <ID> tcp-connect destination <TAB>

HOST-NAME-STR         Hostname of the destination.

IP-ADDR               Destination IPv4 address for the IP SLA.



ArubaOS-Switch(config)# ip-sla <ID> tcp-connect destination 10.22.33.44 <TAB>

 PORT-NUM             Destination port for the IP SLA



ArubaOS-Switch(config)# ip-sla <ID> tcp-connect destination 10.22.33.44 4453 <TAB>

 source               Configure the source IPv4 Address/vlan id for the IP SLA test.

ArubaOS-Switch(config)# portscan-detection timed-block-duration <tab>

 <1-86400>            Enter the timed-block-duration (default is 60 seconds) in which a
triggered client with a timed-block action shall be kept in the blocked state.

ArubaOS-Switch(config)# portscan-detection timed-rate-limit-duration <tab>

<1-86400>             Enter the timed-rate-limit-duration (default is 60 seconds) in which a
triggered client with a timed-rate-limit shall be kept in the rate-limit state

ArubaOS-Switch(config)# portscan-detection reset-host <tab>

       <IP-ADDR>       Define the IP address as the first part of a triggered host ID.
       <VLAN-ID>       Define the VLAN ID as the second part of a triggered host ID.
       all             Removes all hosts that are in a triggered state.
```

Cisco

```
Cisco(Config)#ip sla group schedule group-operation-number operation-id-numbers {schedule-
period schedule-period-range | schedule-together} [ageout seconds] [frequency group-
operation-frequency] [life {forever |seconds}] [start-time {hh:mm [:ss] [month day | day
month] | pending | now | after hh:mm [:ss]}]
```

```
Cisco(Config)#ip sla monitor

Cisco(Config)#auto ip sla mpls-lsp-monitor

Cisco(Config)#ip sla monitor reaction-configuration

Cisco(Config)#auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 frequency 100
start-time now

Cisco(Config)#auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd tree-trace
action-type

Cisco(Config)#auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd lpd-group
retry 3

Cisco(Config)#ip sla ethernet-monitor schedule operation-number schedule-
period seconds [frequency [seconds]] [start-time {afterhh:mm:ss | hh:mm[:ss]
[month day | day month] | now | pending}]

Cisco(Config)#ip sla monitor schedule 99 life 300 start-time after 00:05:00

Cisco(Config)#lives-of-history-kept lives

Cisco(Config)# (config-tplt-tcp-conn)# tos 128

Cisco(Config)# (config)# ip sla auto template type ip tcp-connect 6

Cisco(Config)#ip sla responder tcp-connect ipaddress

Cisco(Config)#ip sla monitor responder type tcpConnect ipaddress

Cisco(Config)#threat-detection rate {acl-drop | bad-packet-drop | conn-limit-drop | dos-drop
| fw-drop | icmp-drop | inspect-drop | interface-drop | scanning-threat | syn-attack} rate-
interval rate_interval average-rate av_rate burst-rate burst_rate

Cisco(Config)#threat-detection scanning-threat shun except ip-address 10.1.1.1
255.255.255.255
```

g) Federal Govt Certification, Netdestination

ArubaOS-Switch	Cisco
ArubaOS-Switch(config)#ntp authentication key-id 1 authentication-mode md5 key-value test trusted	Cisco(config)#ntp authentication-key number md5 *md5-string*
ArubaOS-Switch(config)#aaa authentication ssh login two-factor two-factor-type publickey-password local none	Cisco(config)#aaa authentication login error-enable
ArubaOS-Switch(config)#aaa authentication ssh login two-factor two-factor-type publickey-password radius none	Cisco(config)# aaa authorization config-commands default group tac1
ArubaOS-Switch(config)#crypto pki ta-profile <Profile-Name> ssh-user-name <user-name	Cisco(config)#crypto pki trustpoint name

ArubaOS-Switch(config)#crypto pki create-csr certificate-name <certificate Name> ta-profile <TA profile name> key-type rsa key-size <Key size> usage ssh-server subject	Cisco(ca-trustpoint)# enrollment url http://cat.example.com
ArubaOS-Switch(config)#show authentication two-factor	Cisco(config)#show aaa authentication login error-enable
ArubaOS-Switch(config)#aaa authentication ssh client certificate none	Cisco(config)#aaa authentication login {default | list-name} method1 [method2]
ArubaOS-Switch(config)#crypto pki create-csr certificate-name CERT-NAME ta-profile TA-PROFILE-NAME usage ssh-client subject common-name CN-VALUE	Cisco(config)#crypto pki trustpoint name
ArubaOS-Switch(config)#ip ssh rekey	
ArubaOS-Switch(config)#password non-plaintext-sha256	Cisco(config)# password <password>
ArubaOS-Switch(config)#password manager sha256 <SHA 256 password>	Cisco(config)#config switchconfig strong-pwd {case-check | consecutive-check | default-check | username-check | all-checks} {enable| disable]
ArubaOS-Switch(config)#aaa authentication local-user <username> group <group name> password sha256 <SHA 256 password>	Cisco(config)#aaa common-criteria policy policy1
ArubaOS-Switch(config)#crypto enforce secure-rsa	Cisco(config)#crypto engine accelerator
ArubaOS-Switch(config)#tls application {web-ssl | openflow | syslog | tr69 | cloud | all} lowest-version {tls1.0 | tls 1.1| tls 1.2 | default } [cipher {aes256-sha256 | aes256-sha | aes128-sha256 | aes128-sha | des3-cbc-sha | ecdh-rsa-aes128-gcm-sha256}]	Cisco(config-onep)# transport type tls disable-remotecert-validation
ArubaOS-Switch(config)#Router ospf3 area <area-id> security authentication ipsec spi <spi> md5/sha1 key asci/hex <key-str>	Cisco(config)#ipv6 ospf cost dynamic weight resources 29
ArubaOS-Switch(config)#Vlan <vlan-id> ipv6 ospf3 security authentication ipsec spi <spi> md5/sha1 key asci/hex <key-str>	Cisco(config)#ospfv3 authentication {ipsec spi} {md5 | sha1}{ key-encryption-type key} | null
ArubaOS-Switch(config)#Interface tunnel<id> ipv6 ospf3 security authentication ipsec spi <spi> md5/sha1 key asci/hex <key-str>	Cisco(config)#ipv6 ospf authentication {null | ipsec spi spi authentication-algorithm [key-encryption-type] [key]}
ArubaOS-Switch(config)#Router ospf3 area <area-id> security disable	

ArubaOS-Switch(config)#Vlan <vlan-id> ipv6 ospf3 security disable	Cisco(config)#ipv6 ospf authentication ipsec spi 500 md5 1234567890ABCDEF1234567890ABCD
ArubaOS-Switch(config)#Show crypto ipsec sa ospfv3 ip-address <ip-address>	Cisco(config)#show crypto ipsec sa [map map-name | address | identity] [detail]
ArubaOS-Switch(config)#Show crypto ipsec sa ospfv3 spi <spi>	Cisco(config)#show crypto ipsec security-association lifetime
ArubaOS-Switch(config)#Show crypto ipsec summary ospfv3 ip-address <ip-address>	Cisco(config)#show crypto map [interface interface | tag map-name]
ArubaOS-Switch(config)#show ipv6 ospf3 ipsec summary	Cisco(config)#show ipv6 ospf [process-id] [area-id] [rate-limit]
ArubaOS-Switch(config)#show ipv6 ospf3 security area/interface vlan <id>	Cisco(config)#show ip ospf [process-id] border-routers
ArubaOS-Switch(config)#netdestination [<NAME-STR>] host/network <ip address>	Cisco(config)#ip flow-export destination {ip flow-export destination {hostname | ip-address} udp-port
ArubaOS-Switch(config)#netservice [<NAME-STR>] tcp/udp <port number	Cisco(config)#ip flow-export version 5|9 {origin-as | peer-as}
ArubaOS-Switch(config)#ip access-list standard 1 permit/deny alias-src [<NAME-STR>]	Cisco(config)#show ip flow export
ArubaOS-Switch(config)#Ip access-list extended 100 permit/deny alias-src [<NAME-STR>] alias-dst [<NAME-STR>] alias-srvc [<NAME-STR>]	Cisco(config)#ip flow-export source {{vlan vlan_ID} | {type slot/port} | {port-channel number}| {loopback number}]
ArubaOS-Switch(config)#show net-destination [<NAME-STR>]	Cisco(config)#show ip flow export
ArubaOS-Switch(config)#show net-service [<NAME-STR>]	Cisco(config)#show mls node

Chapter 18 PoE (Power over Ethernet)

This chapter compares the commands used to configure Power over Ethernet (PoE).

PoE is defined in the IEEE 802.3af-2003 standard and enables power-sourcing equipment (PSE) to supply up to 15.4 W of DC power to powered devices (PDs) through Ethernet interfaces over twisted pair cables.

PoE+ is defined in the IEEE 802.3at-2009 standard and supplies up to 25.5W of DC power to each device.

This chapter covers PoE and PoE+ capable devices, but many of the commands are the same for either. See the specific product manuals for further information.

On ArubaOS-Switch and Cisco switches, PoE is enabled by default. On Comware, PoE is disabled by default.

ArubaOS-Switch pre-std-detect is now off. (It was on in previous versions of the software.)

Comware supports nonstandard PDs, referred to as 'poe legacy'. PoE is configured per port.

Cisco autodetects older Cisco pre-standard as well as IEEE-compliant PoE-enabled devices.

ArubaOS-Switch	Comware	Cisco
(PoE enabled by default)	(PoE disabled by default)	(PoE enabled by default) (note, 3750 used for this chapter)
	[Comware-GigabitEthernet1/0/5]poe enable	
ArubaOS-Switch# show power-over-ethernet	[Comware]display poe device	
ArubaOS-Switch# show power-over-ethernet brief	[Comware]display poe interface	Cisco#show power inline
ArubaOS-Switch# show power-over-ethernet 5	[Comware]display poe interface g1/0/5	Cisco#show power inline f1/0/5
ArubaOS-Switch(config)# interface 5	[Comware]interface g1/0/5	Cisco(config)#interface f1/0/5
ArubaOS-Switch(eth-5)# no power-over-ethernet	[Comware-GigabitEthernet1/0/5]undo poe enable	Cisco(config-if)#power inline never
ArubaOS-Switch(eth-5)# power-over-ethernet	[Comware-GigabitEthernet1/0/5]poe enable	Cisco(config-if)#power inline auto
ArubaOS-Switch(config)# rest-interface session-idle-timeout		Cisco(config)# rest-api agent
ArubaOS-Switch(config)# show rest-interface		Cisco(config)# debug rest-api daemon event
ArubaOS-Switch(config)# show system power-supply detailed		Cisco(config)#show system cores

ArubaOS-Switch

```
ArubaOS-Switch# show power-over-ethernet ?
 brief                 Show summary of PoE port configuration and status information.
 [ethernet] PORT-LIST  Show the ports' poe status.
 slot                  Show poe information of specified slot.
 <cr>

ArubaOS-Switch# show power-over-ethernet

 Status and Counters - System Power Status

  System Power Status    : No redundancy
  PoE Power Status       : No redundancy

 Chassis power-over-ethernet:

  Total Available Power  :  573 W
  Total Failover Power   :    0 W
  Total Redundancy Power :    0 W
  Total Used Power       :    8 W +/- 6W
  Total Remaining Power  :  565 W

 Internal Power

        Main Power
  PS    (Watts)        Status
  ----- -------------- ---------------------
  1     573            POE+ Connected
  2     0              Not Connected


ArubaOS-Switch# show power-over-ethernet brief

 Status and Counters - Port Power Status

  System Power Status    : No redundancy
  PoE Power Status       : No redundancy

  Available: 573 W  Used: 8 W  Remaining: 565 W

  Module 1-26 Power
  Available: 573 W  Used: 8 W  Remaining: 565 W

  PoE    | Power  Power    Alloc Alloc Actual Config   Detection   Power Pre-std
  Port   | Enable Priority By    Power Power  Type     Status      Class Detect
  ------ + ------ -------- ----- ----- ------ -------- ----------- ----- ------
  1      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  2      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  3      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  4      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  5      | Yes    low      usage 17 W  7.0 W           Delivering  3     off
  6      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  7      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  8      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  9      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  10     | Yes    low      usage 17 W  0.0 W           Searching   0     off
  11     | Yes    low      usage 17 W  0.0 W           Searching   0     off
  12     | Yes    low      usage 17 W  0.0 W           Searching   0     off
  13     | Yes    low      usage 17 W  0.0 W           Searching   0     off
```

```
  14      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  15      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  16      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  17      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  18      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  19      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  20      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  21      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  22      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  23      | Yes    low      usage 17 W  0.0 W           Searching   0     off
  24      | Yes    low      usage 17 W  0.0 W           Searching   0     off


ArubaOS-Switch# show power-over-ethernet 5

 Status and Counters - Port Power Status for port 5

  Power Enable      : Yes
                                          LLDP Detect       : enabled
  Priority          : low                 Configured Type   :
  AllocateBy        : usage               Value             : 17 W
  Power Class       : 3                   Detection  Status : Delivering

  Over Current Cnt  : 0                   MPS Absent Cnt    : 0
  Power Denied Cnt  : 0                   Short Cnt         : 0

  Voltage           : 54.5 V              Current           : 129 mA
  Power             : 7.0 W               Pre-std Detect    : off


ArubaOS-Switch(config)# interface 5

ArubaOS-Switch(eth-5)# no power-over-ethernet


ArubaOS-Switch# show power-over-ethernet 5

 Status and Counters - Port Power Status for port 5

  Power Enable      : No


ArubaOS-Switch(config)# interface 5


ArubaOS-Switch(eth-5)# power-over-ethernet


ArubaOS-Switch# show power-over-ethernet 5


 Status and Counters - Port Power Status for port 5

  Power Enable      : Yes
                                          LLDP Detect       : enabled
  Priority          : low                 Configured Type   :
  AllocateBy        : usage               Value             : 17 W
  Power Class       : 3                   Detection  Status : Delivering

  Over Current Cnt  : 0                   MPS Absent Cnt    : 0
  Power Denied Cnt  : 0                   Short Cnt         : 0

  Voltage           : 54.5 V              Current           : 97 mA
```

```
  Power              : 5.2 W              Pre-std Detect    : off

ArubaOS-Switch(config)# rest-interface
<tab>

 session-idle-timeout           Set the idle timeout for the REST interface sessions.
```

Comware

Note – PoE disabled by default

```
[Comware]interface g1/0/5

[Comware-GigabitEthernet1/0/5]poe ?
  enable          Port power enable
  max-power       Port maximum power
  pd-description  PD description
  priority        Port power priority

[Comware-GigabitEthernet1/0/5]poe enable ?
  <cr>

[Comware-GigabitEthernet1/0/5]poe enable


[Comware]display poe ?
  device     Available PSE
  interface  Specify the PoE Port
  pse        PSE information

[Comware]display poe device
 PSE ID  SlotNo SubSNo PortNum  MaxPower(W)  State  Model
 4       1      0      24       370          on     PD67024


[Comware]display poe interface
Interface    Status   Priority CurPower Operating  IEEE   Detection
                               (W)      Status     Class  Status
 PSE : 4
 GE1/0/1      disabled low      0.0      off        0      disabled
 GE1/0/2      disabled low      0.0      off        0      disabled
 GE1/0/3      disabled low      0.0      off        0      disabled
 GE1/0/4      disabled low      0.0      off        0      disabled
 GE1/0/5      enabled  low      4.0      on         2      delivering-power
 GE1/0/6      disabled low      0.0      off        0      disabled
 GE1/0/7      disabled low      0.0      off        0      disabled
 GE1/0/8      disabled low      0.0      off        0      disabled
 GE1/0/9      disabled low      0.0      off        0      disabled
 GE1/0/10     disabled low      0.0      off        0      disabled
 GE1/0/11     disabled low      0.0      off        0      disabled
 GE1/0/12     disabled low      0.0      off        0      disabled
 GE1/0/13     disabled low      0.0      off        0      disabled
 GE1/0/14     disabled low      0.0      off        0      disabled
 GE1/0/15     disabled low      0.0      off        0      disabled
 GE1/0/16     disabled low      0.0      off        0      disabled
 GE1/0/17     disabled low      0.0      off        0      disabled
 GE1/0/18     disabled low      0.0      off        0      disabled
 GE1/0/19     disabled low      0.0      off        0      disabled
 GE1/0/20     disabled low      0.0      off        0      disabled
 GE1/0/21     disabled low      0.0      off        0      disabled
 GE1/0/22     disabled low      0.0      off        0      disabled
```

```
 GE1/0/23     disabled low      0.0      off        0      disabled
 GE1/0/24     disabled low      0.0      off        0      disabled

   ---  1 port(s) on,    3.9 (W) consumed,   366.1 (W) remaining ---


[Comware]display poe interface g1/0/5
 Port Power Enabled               : enabled
 Port Power Priority              : low
 Port Operating Status            : on
 Port IEEE Class                  : 2
 Port Detection Status            : delivering-power
 Port Power Mode                  : signal
 Port Current Power               : 4000     mW
 Port Average Power               : 3994     mW
 Port Peak Power                  : 4100     mW
 Port Max Power                   : 15400    mW
 Port Current                     : 79       mA
 Port Voltage                     : 50.4     V
 Port PD Description              :


[Comware]interface g1/0/5

[Comware-GigabitEthernet1/0/5]undo poe enable


[Comware]display poe interface g1/0/5
 Port Power Enabled               : disabled
 Port Power Priority              : low
 Port Operating Status            : off
 Port IEEE Class                  : 0
 Port Detection Status            : disabled
 Port Power Mode                  : signal
 Port Current Power               : 0        mW
 Port Average Power               : 0        mW
 Port Peak Power                  : 0        mW
 Port Max Power                   : 15400    mW
 Port Current                     : 0        mA
 Port Voltage                     : 0.0      V
 Port PD Description              :


[Comware]interface g1/0/5

[Comware-GigabitEthernet1/0/5]poe enable


[Comware]display poe interface g1/0/5
 Port Power Enabled               : enabled
 Port Power Priority              : low
 Port Operating Status            : on
 Port IEEE Class                  : 2
 Port Detection Status            : delivering-power
 Port Power Mode                  : signal
 Port Current Power               : 4000     mW
 Port Average Power               : 3220     mW
 Port Peak Power                  : 4000     mW
 Port Max Power                   : 15400    mW
 Port Current                     : 79       mA
 Port Voltage                     : 50.4     V
 Port PD Description              :
```

Cisco

```
Cisco#show power inline

Module   Available     Used     Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
1           370.0        6.3       363.7
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa1/0/1   auto   off        0.0     n/a                 n/a   15.4
Fa1/0/2   auto   off        0.0     n/a                 n/a   15.4
Fa1/0/3   auto   off        0.0     n/a                 n/a   15.4
Fa1/0/4   auto   off        0.0     n/a                 n/a   15.4
Fa1/0/5   auto   on         6.3     IP Phone 7960       n/a   15.4
Fa1/0/6   auto   off        0.0     n/a                 n/a   15.4
Fa1/0/7   auto   off        0.0     n/a                 n/a   15.4


Cisco#show power inline f1/0/5

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa1/0/5   auto   on         6.3     IP Phone 7960       n/a   15.4

Interface  AdminPowerMax   AdminConsumption
             (Watts)           (Watts)
---------- --------------- --------------------

Fa1/0/5               15.4                 15.4


Cisco(config)#interface f1/0/5

Cisco(config-if)#power inline never


Cisco#show power inline f1/0/5

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa1/0/5   off    off        0.0     n/a                 n/a   15.4

Interface  AdminPowerMax   AdminConsumption
             (Watts)           (Watts)
---------- --------------- --------------------

Fa1/0/5               15.4                 15.4


Cisco(config)#interface f1/0/5

Cisco(config-if)#power inline auto


Cisco#show power inline f1/0/5

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
```

```
--------- ------ ---------- ------- ------------------- ----- ----
Fa1/0/5   auto   on         6.3     IP Phone 7960       n/a   15.4

Interface  AdminPowerMax   AdminConsumption
             (Watts)           (Watts)
---------- --------------- --------------------

Fa1/0/5               15.4                 15.4
```

Chapter 19 VoIP Support

This chapter compares the commands you use to configure Voice over IP (VoIP) operations on VLANs, interfaces, or ports.

These configuration examples support one port that you define for voice as tag/trunk for vlan 230 and data on untagged/access for vlan 220.

The VoIP phone is connected directly to the switch and a client computer is connect directly to the VoIP phone.

ArubaOS-Switch	Comware5	Cisco
	(See notes below about source MAC for voice devices) [Comware5] voice vlan mac-address 001a-a100-0000 mask ffff-ff00-0000 description Cisco-7961	
ArubaOS-Switch(config)# vlan 230	[Comware5]vlan 230	Cisco(config)#vlan 230
ArubaOS-Switch(vlan-230)# voice	[Comware5-vlan230]name voice	Cisco(config-vlan)#name voice
	[Comware5]interface g1/0/5	Cisco(config)#interface g1/0/5
	[Comware5-GigabitEthernet1/0/5]port link-type access [Comware5-GigabitEthernet1/0/5]port link-type hybrid	Cisco(config-if)#switchport
ArubaOS-Switch(vlan-230)# vlan 220 ArubaOS-Switch(vlan-220)# untagged 5	[Comware5-GigabitEthernet1/0/5]port hybrid vlan 220 untagged [Comware5-GigabitEthernet1/0/5]port hybrid pvid vlan 220	Cisco(config-if)#switchport access vlan 220
		Cisco(config-if)#switchport mode access
ArubaOS-Switch(vlan-220)# vlan 230 ArubaOS-Switch(vlan-230)# tagged 5	[Comware5-GigabitEthernet1/0/5]voice vlan 230 enable	Cisco(config-if)#switchport voice vlan 230
	[Comware5-GigabitEthernet1/0/5]poe enable	
ArubaOS-Switch# show vlans 230	<Comware5>display vlan 230	
ArubaOS-Switch# show vlan ports 5 detail	<Comware5>display interface g1/0/5	Cisco#show interfaces g1/0/5 switchport
	<Comware5>display voice vlan state	

	<Comware5>display voice vlan oui	
	Comware7	
	(See notes below about source MAC for voice devices) [Comware7] voice-vlan mac-address 0013-6000-0000 mask ffff-ff00-0000 description Cisco-7960	
	[Comware7]vlan 230	
	[Comware7-vlan230]name voice	
	[Comware7]interfaceg1/0/5	
	[Comware7-GigabitEthernet1/0/5]port link-type access [Comware7-GigabitEthernet1/0/5]port link-type hybrid	
	[Comware7-GigabitEthernet1/0/5]port hybrid vlan 220 untagged [Comware7-GigabitEthernet1/0/5]port hybrid pvid vlan 220	
	[Comware7-GigabitEthernet1/0/5]voice vlan 230 enable	
	[Comware7-GigabitEthernet1/0/5]poe enable	
	<Comware7>display vlan 230	
	<Comware7>display interface g1/0/5	
	<Comware7>display voice-vlan state	
	<Comware7>display voice-vlan mac-address	

ArubaOS-Switch

```
ArubaOS-Switch(config)# vlan 230

ArubaOS-Switch(vlan-230)# voice

ArubaOS-Switch(vlan-230)# vlan 220

ArubaOS-Switch(vlan-220)# untagged 5

ArubaOS-Switch(vlan-220)# vlan 230

ArubaOS-Switch(vlan-230)# tagged 5
```

```
ArubaOS-Switch# show vlans 230

 Status and Counters - VLAN Information - VLAN 230

  VLAN ID : 230
  Name : voice
  Status : Port-based
  Voice : Yes
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  5                Tagged   Learn        Up


ArubaOS-Switch# show vlan ports 5 detail

 Status and Counters - VLAN Information - for ports 5

  VLAN ID Name                 | Status     Voice Jumbo Mode
  ------- -------------------- + ---------- ----- ----- --------
  220     test                 | Port-based No    No    Untagged
  230     voice                | Port-based Yes   No    Tagged
```

Comware5

Comware determines whether a received packet is a voice packet by checking its source MAC address. There are a few built-in preconfigured OUI addresses defined in Comware, but as there are many newer voice capable devices on the market, generally additional MAC address prefix definitions may be required. We show the addition of one such MAC prefix in this example configuration.

```
[Comware5]voice ?
  vlan  Specify voice VLAN

[Comware5]voice vlan ?
  aging        Aging time
  mac-address  MAC Address
  security     Specify voice VLAN security mode
  track        Learn oui from lldp

[Comware5]voice vlan mac-address ?
  H-H-H  MAC address

[Comware5]voice vlan mac-address 001a-a100-0000 ?
  mask  MAC address mask

[Comware5]voice vlan mac-address 001a-a100-0000 mask ffff-ff00-0000 ?
  description  MAC address description
  <cr>

[Comware5]voice vlan mac-address 001a-a100-0000 mask ffff-ff00-0000 description ?
  TEXT  MAC address description(up to 30 characters)

[Comware5]voice vlan mac-address 001a-a100-0000 mask ffff-ff00-0000 description Cisco-7961 ?
   TEXT
   <cr>

[Comware5]voice vlan mac-address 001a-a100-0000 mask ffff-ff00-0000 description Cisco-7961


[Comware5]vlan 230

[Comware5-vlan230]name voice
```

```
[Comware5]interface g1/0/5

[Comware5-GigabitEthernet1/0/5]port link-type access

[Comware5-GigabitEthernet1/0/5]port link-type hybrid

[Comware5-GigabitEthernet1/0/5]port hybrid vlan 220 untagged

[Comware5-GigabitEthernet1/0/5]port hybrid pvid vlan 220

[Comware5-GigabitEthernet1/0/5]voice vlan 230 enable

[Comware5-GigabitEthernet1/0/5]poe enable


<Comware5>display vlan 230
VLAN ID: 230
 VLAN Type: static
 Route Interface: configured
 IPv4 address: 10.1.230.3
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0230
 Name: voice
 Tagged   Ports:
    GigabitEthernet1/0/5
 Untagged Ports: none


<Comware5>display interface g1/0/5
 GigabitEthernet1/0/5 current state: UP
...
 PVID: 220
 Mdi type: auto
 Port link-type: hybrid
  Tagged   VLAN ID : 230
  Untagged VLAN ID : 100, 220
...


<Comware5>display voice vlan state
 Maximum of Voice VLANs: 8
 Current Voice VLANs: 1
 Voice VLAN security mode: Security
 Voice VLAN aging time: 1440 minutes
 Voice VLAN enabled port and its mode:
 PORT                        VLAN        MODE        COS        DSCP
 ------------------------------------------------------------------
 GigabitEthernet1/0/5        230         AUTO        6          46


<Comware5>display voice vlan oui
Oui Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
001a-a100-0000  ffff-ff00-0000  Cisco-7961
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3com phone
```

Comware7

Comware determines whether a received packet is a voice packet by checking its source MAC address. There are a few built-in preconfigured OUI addresses defined in Comware, but as there are many newer voice capable devices on the market, generally additional MAC address prefix definitions may be required. We show the addition of one such MAC prefix in this example configuration.

```
[Comware7]voice-vlan ?
  aging        Specify aging time
  mac-address  Specify MAC address
  security     Voice VLAN security mode
  track        Learn OUI from LLDP

[Comware7]voice-vlan mac-address ?
  H-H-H  MAC Address

[Comware7]voice-vlan mac-address 0013-6000-0000 ?
  mask  Specify MAC address mask

[Comware7]voice-vlan mac-address 0013-6000-0000 mask ffff-ff00-0000 ?
  description  Specify MAC address description
  <cr>

[Comware7]voice-vlan mac-address 0013-6000-0000 mask ffff-ff00-0000 description
Cisco-7960 ?
  TEXT  MAC address description (of up to 30 characters)
  <cr>

[Comware7]voice-vlan mac-address 0013-6000-0000 mask ffff-ff00-0000 description Cisco-7960


[Comware7]vlan 230

[Comware7-vlan230]name voice


[Comware7]interface g1/0/5

[Comware7-GigabitEthernet1/0/5]port link-type access

[Comware7-GigabitEthernet1/0/5]port link-type hybrid

[Comware7-GigabitEthernet1/0/5]port hybrid vlan 220 untagged

[Comware7-GigabitEthernet1/0/5]port hybrid pvid vlan 220

[Comware7-GigabitEthernet1/0/5]voice-vlan 230 enable

[Comware7-GigabitEthernet1/0/5]poe enable


<Comware7>display vlan 230
 VLAN ID: 230
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 10.1.230.5
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0230
 Name: voice
 Tagged ports:
    GigabitEthernet1/0/5
 Untagged ports: None
```

```
<Comware7>display interface g1/0/5
GigabitEthernet1/0/5
Current state: UP
...
PVID: 220
MDI type: automdix
Port link-type: Hybrid
 Tagged VLANs:   230
 Untagged VLANs: 100, 220
...


<Comware7>display voice-vlan state
 Current voice VLANs: 1
 Voice VLAN security mode: Security
 Voice VLAN aging time: 1440 minutes
 Voice VLAN enabled ports and their modes:
 Port                        VLAN        Mode        CoS         DSCP
 GigabitEthernet1/0/5        230         AUTO        6           46


<Comware7>display voice-vlan mac-address
OUI Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
000f-e200-0000  ffff-ff00-0000  H3C Aolynk phone
0013-6000-0000  ffff-ff00-0000  Cisco-7960
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3Com phone
```

Cisco

```
Cisco(config)#vlan 230

Cisco(config-vlan)#name voice


Cisco(config)#interface g1/0/5

Cisco(config-if)#switchport

Cisco(config-if)#switchport access vlan 220

Cisco(config-if)#switchport mode access

Cisco(config-if)#switchport voice vlan 230


Cisco#show interfaces g1/0/5 switchport
Name: Gi1/0/5
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 220 (test)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
```

```
Voice VLAN: 230 (voice)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Chapter 20 Link Aggregation – LACP and Trunk

This chapter compares the commands you use to configure aggregation interfaces.

The IEEE 802.3ad Link Aggregation Control Protocol (LACP) enables dynamic aggregation of physical links. It uses Link Aggregation Control Protocol Data Units (LACPDUs) to exchange aggregation information between LACP-enabled devices.

There are some terminology differences among the operating systems for the terms used to define port aggregation. In ArubaOS-Switch, aggregated links are called *trunks*. In Comware , the term is *bridge aggregation*; in Cisco it is *EtherChannel*. In addition, Cisco Etherchannel has two modes: PAgP (Cisco specific) or LACP. LACP mode is shown in the Cisco configuration examples.

In Comware and Cisco, *trunk* refers to an interface that is configured to support multiple VLANs via 802.1Q.

This chapter covers the configuration of LACP port aggregation—sometimes referred to as protocol trunks, which are dynamic in their operation—and non-LACP port aggregation, sometimes referred to as non-protocol trunks, which are basically "on," because no protocol is used to negotiate the aggregated links.

Generally, execute the configuration steps first then connect the links -or- disable/shutdown the interfaces, execute the configuration steps, then enable/undo or no shutdown the interfaces. Otherwise network loops could accidently be created and cause other issues/outages.

a) Link Aggregation Control Protocol (LACP)

ArubaOS-Switch	Comware	Cisco
`ArubaOS-Switch(config)# trunk 20-23 trk1 lacp`	`[Comware]interface Bridge-Aggregation 1`	`Cisco(config)#interface port-channel 1`
`ArubaOS-Switch(config)# vlan 220 tagged trk1`	`[Comware-Bridge-Aggregation1]description LACP-link-to-ArubaOS-Switch`	`Cisco(config-if)#switchport trunk encapsulation dot1q`
	`[Comware-Bridge-Aggregation1]link-aggregation mode dynamic`	`Cisco(config-if)#switchport trunk allowed vlan 220`
	`[Comware]interface g1/0/23`	`Cisco(config-if)#switchport mode access`
	`[Comware-GigabitEthernet1/0/23]port link-aggregation group 1`	`Cisco(config-if)#switchport nonegotiate`
	`[Comware-GigabitEthernet1/0/23]interface g1/0/24`	`Cisco(config)#interface range g1/0/23 - 24`
	`[Comware-GigabitEthernet1/0/24]port link-aggregation group 1`	`Cisco(config-if-range)#switchport trunk encapsulation dot1q`
	`[Comware]interface Bridge-Aggregation 1`	`Cisco(config-if-range)#switchport trunk allowed vlan 220`
	`[Comware-Bridge-Aggregation1]port link-type trunk`	`Cisco(config-if-range)#switchport mode access`

	[Comware-Bridge-Aggregation1]port trunk permit vlan 220	Cisco(config-if-range)#switchport nonegotiate
		Cisco(config-if-range)#channel-group 1 mode active
ArubaOS-Switch# show trunks ArubaOS-Switch# show lacp	[Comware]display link-aggregation summary	Cisco#show lacp 1 internal
ArubaOS-Switch# show lacp peer	[Comware]display link-aggregation verbose	
ArubaOS-Switch# show lacp peer ArubaOS-Switch# show lacp counters	[Comware]display link-aggregation member-port	Cisco#show interfaces etherchannel
ArubaOS-Switch# show vlans 220 ArubaOS-Switch# show vlans ports trk1 detail	[Comware]display vlan 220	Cisco#show vlan name test

ArubaOS-Switch

```
ArubaOS-Switch(config)# trunk 19-20 trk1 lacp


ArubaOS-Switch(config)# vlan 220 tagged trk1


ArubaOS-Switch# show trunks

Load Balancing Method:  L3-based (default)

  Port   | Name                              Type      | Group  Type
  ------ + --------------------------------- --------- + ------ --------
  19     | trk1-link-to-Comware5-1           100/1000T | Trk1   LACP
  20     | trk1-link-to-Comware5-1           100/1000T | Trk1   LACP
  21     | trk2-link-to-Comware7-1           100/1000T | Trk2   LACP
  22     | trk2-link-to-Comware7-1           100/1000T | Trk2   LACP
  23     | trk3-link-to-Cisco1               100/1000T | Trk3   LACP
  24     | trk3-link-to-Cisco1               100/1000T | Trk3   LACP


ArubaOS-Switch# show lacp

                                   LACP

           LACP      Trunk     Port                LACP      Admin   Oper
   Port    Enabled   Group     Status    Partner   Status    Key     Key
   -----   -------   -------   -------   -------   -------   ------  ------
   19      Active    Trk1      Up        Yes       Success   0       562
   20      Active    Trk1      Up        Yes       Success   0       562
   21      Active    Trk2      Up        Yes       Success   0       563
   22      Active    Trk2      Up        Yes       Success   0       563
   23      Active    Trk3      Up        Yes       Success   0       564
   24      Active    Trk3      Up        Yes       Success   0       564


ArubaOS-Switch# show lacp peer
```

```
LACP Peer Information.


System ID: 009c02-d53980


  Local  Local                        Port      Oper    LACP     Tx
  Port   Trunk  System ID      Port  Priority  Key     Mode     Timer
  ------ ------ -------------- ----- --------- ------- -------- -----
  19     Trk1   002389-d5a059  23    32768     1       Active   Slow
  20     Trk1   002389-d5a059  24    32768     1       Active   Slow
  21     Trk2   cc3e5f-73bacb  23    32768     1       Active   Slow
  22     Trk2   cc3e5f-73bacb  24    32768     1       Active   Slow
  23     Trk3   002291-ab4380  280   32768     1       Active   Slow
  24     Trk3   002291-ab4380  281   32768     1       Active   Slow


ArubaOS-Switch# show lacp counters

LACP Port Counters.


              LACP      LACP      Marker   Marker   Marker   Marker
  Port Trunk  PDUs Tx   PDUs Rx   Req. Tx  Req. Rx  Resp. Tx Resp. Rx Error
  ---- ------ --------- --------- -------- -------- -------- -------- --------
  19   Trk1   19        18        0        0        0        0        0
  20   Trk1   18        17        0        0        0        0        0
  21   Trk2   41        40        0        0        0        0        0
  22   Trk2   40        39        0        0        0        0        0
  23   Trk3   8         8         0        0        0        0        0
  24   Trk3   8         8         0        0        0        0        0


ArubaOS-Switch# show vlans 220

 Status and Counters - VLAN Information - VLAN 220

  VLAN ID : 220
  Name : test
  Status : Port-based
  Voice : No
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  4                Untagged Learn        Down
  5                Untagged Learn        Down
  6                Tagged   Learn        Down
  7                Tagged   Learn        Down
  8                Tagged   Learn        Down
  Trk1             Tagged   Learn        Up
  Trk2             Tagged   Learn        Up
  Trk3             Tagged   Learn        Up


ArubaOS-Switch# show vlans ports trk1 detail

 Status and Counters - VLAN Information - for ports Trk1

  VLAN ID Name                 | Status     Voice Jumbo Mode
  ------- -------------------- + ---------- ----- ----- --------
  1       DEFAULT_VLAN         | Port-based No    No    Untagged
```

```
  220     test                  | Port-based No    No    Tagged
```

Comware

```
[Comware]interface Bridge-Aggregation 1

[Comware-Bridge-Aggregation1]description LACP-link-to-ArubaOS-Switch

[Comware-Bridge-Aggregation1]link-aggregation mode dynamic

[Comware]interface g1/0/23

[Comware-GigabitEthernet1/0/23]port link-aggregation group 1

[Comware-GigabitEthernet1/0/23]interface g1/0/24

[Comware-GigabitEthernet1/0/24]port link-aggregation group 1

[Comware]interface Bridge-Aggregation 1

[Comware-Bridge-Aggregation1]port link-type trunk

[Comware-Bridge-Aggregation1]port trunk permit vlan 220


[Comware]display link-aggregation summary
Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 0023-89d5-a059

AGG         AGG       Partner ID               Select Unselect   Share
Interface   Mode                               Ports  Ports      Type
--------------------------------------------------------------------------------
BAGG1       D         0x3980, 009c-02d5-3980   2      0          Shar


[Comware]display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 0023-89d5-a059
Local:
  Port             Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/0/23         S       32768    1         {ACDEF}
  GE1/0/24         S       32768    1         {ACDEF}
Remote:
```

```
  Actor            Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/0/23         19      0        562       0x3980, 009c-02d5-3980 {ACDEF}
  GE1/0/24         20      0        562       0x3980, 009c-02d5-3980 {ACDEF}


[Comware]display link-aggregation member-port
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/23:
Aggregation Interface: Bridge-Aggregation1
Local:
    Port Number: 23
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Remote:
    System ID: 0x3980, 009c-02d5-3980
    Port Number: 19
    Port Priority: 0
    Oper-Key: 562
    Flag: {ACDEF}
Received LACP Packets: 12 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 12 packet(s)

GigabitEthernet1/0/24:
Aggregation Interface: Bridge-Aggregation1
Local:
    Port Number: 24
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Remote:
    System ID: 0x3980, 009c-02d5-3980
    Port Number: 20
    Port Priority: 0
    Oper-Key: 562
    Flag: {ACDEF}
Received LACP Packets: 11 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 11 packet(s)


[Comware]display vlan 220
VLAN ID: 220
 VLAN Type: static
 Route Interface: configured
 IPv4 address: 10.1.220.3
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0220
 Name: test
```

```
 Tagged   Ports:
    Bridge-Aggregation1
    GigabitEthernet1/0/6     GigabitEthernet1/0/23    GigabitEthernet1/0/24
 Untagged Ports:
    GigabitEthernet1/0/4     GigabitEthernet1/0/5
```

Cisco

```
Cisco(config)#interface port-channel 1

Cisco(config-if)#switchport trunk encapsulation dot1q

Cisco(config-if)#switchport trunk allowed vlan 220

Cisco(config-if)#switchport mode access

Cisco(config-if)#switchport nonegotiate


Cisco(config)#interface range g1/0/24 - 24

Cisco(config-if-range)#switchport trunk encapsulation dot1q

Cisco(config-if-range)#switchport trunk allowed vlan 220

Cisco(config-if-range)#switchport mode access

Cisco(config-if-range)#switchport nonegotiate

Cisco(config-if-range)#channel-group 1 mode active


Cisco#show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Fa1/0/22  SA      bndl      32768         0x1       0x1     0x18        0x3D
Fa1/0/23  SA      bndl      32768         0x1       0x1     0x19        0x3D


Cisco#show interfaces etherchannel
----
GigabitEthernet1/0/23:
Port state    = Up Mstr Assoc In-Bndl
Channel group = 1           Mode = Active          Gcchange = -
Port-channel  = Po1         GC   =   -             Pseudo port-channel = Po1
Port index    = 0           Load = 0x00            Protocol =   LACP

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Gi1/0/23  SA      bndl      32768         0x1       0x1     0x118       0x3D

Partner's information:

                  LACP port                        Admin  Oper   Port    Port
```

```
Port      Flags   Priority  Dev ID          Age    key    Key    Number  State
Gi1/0/23  SA      0         009c.02d5.3980  19s    0x0    0x234  0x17    0x3D

Age of the port in the current state: 0d:00h:03m:16s

----
GigabitEthernet1/0/24:
Port state    = Up Mstr Assoc In-Bndl
Channel group = 1           Mode = Active          Gcchange = -
Port-channel  = Po1         GC   =   -             Pseudo port-channel = Po1
Port index    = 0           Load = 0x00            Protocol =   LACP

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Gi1/0/24  SA      bndl      32768         0x1       0x1     0x119       0x3D

Partner's information:

                  LACP port                        Admin  Oper   Port    Port
Port      Flags   Priority  Dev ID          Age    key    Key    Number  State
Gi1/0/24  SA      0         009c.02d5.3980  13s    0x0    0x234  0x18    0x3D

Age of the port in the current state: 0d:00h:03m:09s

----
Port-channel1:Port-channel1   (Primary aggregator)

Age of the Port-channel   = 0d:00h:06m:29s
Logical slot/port   = 10/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Port security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi1/0/23 Active             0
  0     00     Gi1/0/24 Active             0

Time since last port bundled:    0d:00h:03m:09s    Gi1/0/24


Cisco#show vlan name test

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
220  test                             active    Gi1/0/4, Gi1/0/5

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
220  enet  100220     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
```

```
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- -------------------------------------------
```

b) Trunk

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# trunk 19-20 trk1 trunk	[Comware]interface Bridge-Aggregation 1	Cisco(config)#interface port-channel 1
ArubaOS-Switch(config)# vlan 220 tagged trk1	[Comware-Bridge-Aggregation1]description Trunk-link-to-ArubaOS-Switch	Cisco(config-if)#switchport trunk encapsulation dot1q
	[Comware]interface g1/0/23	Cisco(config-if)#switchport trunk allowed vlan 220
	[Comware-GigabitEthernet1/0/23]port link-aggregation group 1	Cisco(config-if)#switchport mode access
	[Comware-GigabitEthernet1/0/23]interface g1/0/24	Cisco(config-if)#switchport nonegotiate
	[Comware-GigabitEthernet1/0/24]port link-aggregation group 1	Cisco(config)#interface range g1/0/23 - 24
	[Comware]interface Bridge-Aggregation 1	Cisco(config-if-range)#switchport trunk encapsulation dot1q
	[Comware-Bridge-Aggregation1]port link-type trunk	Cisco(config-if-range)#switchport trunk allowed vlan 220
	[Comware-Bridge-Aggregation1]port trunk permit vlan 220	Cisco(config-if-range)#switchport mode access
		Cisco(config-if-range)#switchport nonegotiate
		Cisco(config-if-range)#channel-group 1 mode on
ArubaOS-Switch# show trunks	[Comware]display link-aggregation summary	
	[Comware]display link-aggregation verbose	Cisco#show etherchannel 1 summary
	[Comware]display link-aggregation member-port	Cisco#show interfaces etherchannel
ArubaOS-Switch# show vlans 220 ArubaOS-Switch# show vlans ports trk1 detail	[Comware]display vlan 220	Cisco#show vlan name test

ArubaOS-Switch

```
ArubaOS-Switch(config)# trunk 19-20 trk1 trunk


ArubaOS-Switch(config)# vlan 220 tagged trk1


ArubaOS-Switch# show trunks

Load Balancing Method:  L3-based (default)

  Port    | Name                             Type       | Group  Type
  ------ + -------------------------------- --------- + ------ --------
```

```
  19     | trk1-link-to-Comware5-1          100/1000T | Trk1   Trunk
  20     | trk1-link-to-Comware5-1          100/1000T | Trk1   Trunk
  21     | trk2-link-to-Comware7-1          100/1000T | Trk2   Trunk
  22     | trk2-link-to-Comware7-1          100/1000T | Trk2   Trunk
  23     | trk3-link-to-Cisco1              100/1000T | Trk3   Trunk
  24     | trk3-link-to-Cisco1              100/1000T | Trk3   Trunk


ArubaOS-Switch# show vlans 220

 Status and Counters - VLAN Information - VLAN 220

  VLAN ID : 220
  Name : test
  Status : Port-based
  Voice : No
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  4                Untagged Learn        Down
  5                Untagged Learn        Down
  6                Tagged   Learn        Down
  7                Tagged   Learn        Down
  8                Tagged   Learn        Down
  Trk1             Tagged   Learn        Up
  Trk2             Tagged   Learn        Up
  Trk3             Tagged   Learn        Up


ArubaOS-Switch# show vlans ports trk1 detail

 Status and Counters - VLAN Information - for ports Trk1

  VLAN ID Name                 | Status     Voice Jumbo Mode
  ------- -------------------- + ---------- ----- ----- --------
  1       DEFAULT_VLAN         | Port-based No    No    Untagged
  220     test                 | Port-based No    No    Tagged
```

Comware

```
[Comware]interface Bridge-Aggregation 1

[Comware-Bridge-Aggregation1]description Trunk-link-to-ArubaOS-Switch

[Comware]interface g1/0/23

[Comware-GigabitEthernet1/0/23]port link-aggregation group 1

[Comware-GigabitEthernet1/0/23]interface g1/0/24

[Comware-GigabitEthernet1/0/24]port link-aggregation group 1

[Comware]interface Bridge-Aggregation 1

[Comware-Bridge-Aggregation1]port link-type trunk

[Comware-Bridge-Aggregation1]port trunk permit vlan 220


[Comware]display link-aggregation summary
Aggregation Interface Type:
```

```
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 0023-89d5-a059

AGG         AGG       Partner ID               Select Unselect   Share
Interface   Mode                               Ports  Ports      Type
--------------------------------------------------------------------------------
BAGG1       S         none                     2      0          Shar


[Comware]display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority  Oper-Key
--------------------------------------------------------------------------------
  GE1/0/23         S       32768     1
  GE1/0/24         S       32768     1


[Comware]dis link-aggregation member-port
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/23:
Aggregation Interface: Bridge-Aggregation1
Port Number: 23
Port Priority: 32768
Oper-Key: 1

GigabitEthernet1/0/24:
Aggregation Interface: Bridge-Aggregation1
Port Number: 24
Port Priority: 32768
Oper-Key: 1


[Comware]display vlan 220
VLAN ID: 220
 VLAN Type: static
 Route Interface: configured
 IPv4 address: 10.1.220.3
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0220
 Name: test
 Tagged   Ports:
    Bridge-Aggregation1
    GigabitEthernet1/0/6     GigabitEthernet1/0/23    GigabitEthernet1/0/24
 Untagged Ports:
    GigabitEthernet1/0/4     GigabitEthernet1/0/5
```

Cisco

```
Cisco(config)#interface port-channel 1

Cisco(config-if)#switchport trunk encapsulation dot1q

Cisco(config-if)#switchport trunk allowed vlan 220

Cisco(config-if)#switchport mode access

Cisco(config-if)#switchport nonegotiate


Cisco(config)#interface range g1/0/23 - 24

Cisco(config-if-range)#switchport trunk encapsulation dot1q

Cisco(config-if-range)#switchport trunk allowed vlan 220

Cisco(config-if-range)#switchport mode access

Cisco(config-if-range)#switchport nonegotiate

Cisco(config-if-range)#channel-group 1 mode on


Cisco#show etherchannel 1 summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)          -        Gi1/0/23(P) Gi1/0/24(P)


Cisco#show interfaces etherchannel
----
GigabitEthernet1/0/23:
Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = On              Gcchange = -
Port-channel  = Po1         GC   =   -             Pseudo port-channel = Po1
Port index    = 0           Load = 0x00            Protocol =    -

Age of the port in the current state: 0d:00h:01m:53s

----
GigabitEthernet1/0/24:
Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = On              Gcchange = -
Port-channel  = Po1         GC   =   -             Pseudo port-channel = Po1
Port index    = 0           Load = 0x00            Protocol =    -
```

```
Age of the port in the current state: 0d:00h:01m:51s

----
Port-channel1:
Age of the Port-channel   = 0d:01h:29m:27s
Logical slot/port   = 10/1          Number of ports = 2
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =    -
Port security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi1/0/23 On                 0
  0     00     Gi1/0/24 On                 0

Time since last port bundled:    0d:00h:01m:52s    Gi1/0/24
Time since last port Un-bundled: 0d:00h:37m:22s    Gi1/0/24


Cisco#show vlan name test

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
220  test                             active    Gi1/0/4, Gi1/0/5

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
220  enet  100220     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Chapter 21 RSTP

Based on the IEEE 802.1w standard, Rapid Spanning Tree Protocol (RSTP) is an optimized version of the IEEE 802.1D standard, Spanning Tree Protocol (STP). It achieves rapid network convergence by allowing a newly elected root port or designated port to enter the forwarding state much quicker under certain conditions than STP.

Although RSTP supports rapid network convergence, it has the same drawback as STP: All bridges within a LAN share the same spanning tree, so redundant links cannot be blocked based on VLAN, and the packets of all VLANs are forwarded along the same spanning tree.

This chapter compares the commands you use to configure RSTP. The four operating systems implement RSTP differently:

- ArubaOS-Switch supports RSTP, but Multiple STP (MSTP) is the default STP version. MSTP *is not enabled by default*. When MSTP is enabled, all ports are auto-edge-ports.
- Comware5 supports RSTP, but MSTP is the default STP version. MSTP *is not enabled by default*. When MSTP is enabled, all ports are non-edge ports.
- Comware7 supports RSTP, but MSTP is the default STP version. MSTP *is enabled by default*. When MSTP is enabled, all ports are non-edge ports.
- Cisco uses per-VLAN spanning-tree plus (PVST+) as the default STP version, and it *is enabled by default*. Cisco does not support RSTP (only) as an STP option.

ArubaOS-Switch	Comware5	Cisco
`ArubaOS-Switch(config)# spanning-tree`	`[Comware5]stp enable`	(Not an available feature)
`ArubaOS-Switch(config)# spanning-tree force-version rstp-operation`	`[Comware5]stp mode rstp`	
`ArubaOS-Switch(config)# spanning-tree priority 2`	`[Comware5]stp priority 12288`	
	`[Comware5]interface g1/0/4`	
`ArubaOS-Switch(config)# spanning-tree 4 admin-edge-port`	`[Comware5-GigabitEthernet1/0/4]stp edged-port enable`	
`ArubaOS-Switch(config)# spanning-tree 4 path-cost 10000`	`[Comware5-GigabitEthernet1/0/4]stp cost 10000`	
`ArubaOS-Switch(config)# spanning-tree 4 priority 6`	`[Comware5-GigabitEthernet1/0/4]stp port priority 96`	
`ArubaOS-Switch# show spanning-tree`	`[Comware5]display stp`	
	`[Comware5]display stp brief`	
	Comware7	
	`[Comware7]stp mode rstp`	
	`[Comware7]stp priority 16384`	

	[Comware7]interface g1/0/4	
	[Comware7-GigabitEthernet1/0/4]stp edged-port enable	
	[Comware7-GigabitEthernet1/0/4]stp cost 10000	
	[Comware7-GigabitEthernet1/0/4]stp port priority 96	
	[Comware7]display stp	
	[Comware7]display stp brief	

ArubaOS-Switch

```
ArubaOS-Switch(config)# spanning-tree ?
 bpdu-protection-ti... Set the time for protected ports to be in down state after
                       receiving unauthorized BPDUs.
 bpdu-throttle         Configure BPDU throttling on the device.
 clear-debug-counters  Clear spanning tree debug counters.
 config-name           Set the MST region configuration name (default is switch's MAC
                       address).
 config-revision       Set the MST region configuration revision number (default is 0).
 enable                Enable spanning-tree.
 disable               Disable spanning-tree.
 extend                Enable the extended system ID feature.
 force-version         Set Spanning Tree protocol compatibility mode.
 forward-delay         Set time the switch waits between transitioning from listening to
                       learning and from learning to forwarding states. Not applicable in
                       RPVST mode.
 hello-time            Set time between messages transmission when the switch is root.
                       Not applicable in RPVST mode.
 ignore-pvid-incons... Ignore PVID inconsistencies, allowing Rapid PVST to run on
                       mismatched links.
 instance              Create, delete or configure an MST instance.
 legacy-mode           Set spanning-tree protocol to operate either in 802.1D legacy mode
                       or in 802.1s native mode.
 legacy-path-cost      [Deprecated] Set 802.1D (legacy) or 802.1t (current) default
                       pathcost values.
 log                   Enable event logging for port state transition information.
 max-hops              Set the max number of hops in a region before the MST BPDU is
                       discarded and the information held for a port is aged (default is
                       20).
 maximum-age           Set maximum age of received STP information before it is
                       discarded. Not applicable in RPVST mode.
 mode                  Specify spanning-tree mode.
 pathcost              Specify a standard to use when calculating the default pathcost.
 pending               Manipulate pending MSTP configuration.
 port                  Configure port specific RPVST parameters for the specified VLANs.
 [ethernet] PORT-LIST  Configure the port-specific parameters of the spanning tree
                       protocol for individual ports.
 priority              Set the device STP priority (the value is in range of 0-61440
                       divided into steps of 4096 that are numbered from 0 to 15, default
                       is step 8). Not applicable in RPVST mode.
 root                  Configure root for STP.
 trap                  Enable/disable STP/MSTP/RPVST traps.
 vlan                  Specify RPVST VLAN specific parameters.
 <cr>
```

```
ArubaOS-Switch(config)# spanning-tree

ArubaOS-Switch(config)# spanning-tree  force-version ?
 stp-compatible        The protocol operates as STP on all ports.
 rstp-operation        The protocol operates as Rapid STP on all ports except those ports
                       where a system that is using 802.1d Spanning Tree has been
                       detected.
 mstp-operation        The protocol operates as Multiple STP on all ports where
                       compatibility to the old STP protocol versions is not required.

ArubaOS-Switch(config)# spanning-tree  force-version rstp-operation ?
 bpdu-protection-ti... Set the time for protected ports to be in down state after
                       receiving unauthorized BPDUs.
 forward-delay         Set time the switch waits between transitioning from listening to
                       learning and from learning to forwarding states. Not applicable in
                       RPVST mode.
 hello-time            Set time between messages transmission when the switch is root.
                       Not applicable in RPVST mode.
 max-hops              Set the max number of hops in a region before the MST BPDU is
                       discarded and the information held for a port is aged (default is
                       20).
 maximum-age           Set maximum age of received STP information before it is
                       discarded. Not applicable in RPVST mode.
 priority              Set the device STP priority (the value is in range of 0-61440
                       divided into steps of 4096 that are numbered from 0 to 15, default
                       is step 8). Not applicable in RPVST mode.
 root                  Configure root for STP.
 <cr>

ArubaOS-Switch(config)# spanning-tree force-version rstp-operation

ArubaOS-Switch(config)# spanning-tree priority 2
   (note - multiplier is 4096, default setting is 8)

ArubaOS-Switch(config)# spanning-tree 4 ?
 admin-edge-port       Set the administrative edge port status.
 auto-edge-port        Set the automatic edge port detection.
 bpdu-filter           Stop a specific port or ports from transmitting BPDUs, receiving
                       BPDUs, and assume a continuous fowarding state.
 bpdu-protection       Disable the specific port or ports if the port(s) receives STP
                       BPDUs.
 hello-time            Set message transmission interval (in sec.) on the port. Not
                       applicable in RPVST mode.
 loop-guard            Set port to guard against the loop and consequently to prevent it
                       from becoming Forwarding Port.
 mcheck                Force the port to transmit RST BPDUs. Not applicable in RPVST
                       mode.
 path-cost             Set port's path cost value. Not applicable in RPVST mode.
 point-to-point-mac    Set the administrative point-to-point status.
 priority              Set port priority (the value is in range of 0-240 divided into
                       steps of 16 that are numbered from 0 to 15, default is step 8).
                       Not applicable in RPVST mode.
 pvst-filter           Stop a specific port or ports from receiving and retransmitting
                       PVST BPDUs. Not applicable in RPVST mode.
 pvst-protection       Disable the specific port or ports if the port(s) receives PVST
                       BPDUs. Not applicable in RPVST mode.
 root-guard            Set port to ignore superior BPDUs to prevent it from becoming Root
                       Port.
 tcn-guard             Set port to stop propagating received topology changes
                       notifications and topology changes to other ports.

ArubaOS-Switch(config)# spanning-tree 4 admin-edge-port
```

```
ArubaOS-Switch(config)# spanning-tree 4 path-cost 10000

ArubaOS-Switch(config)# spanning-tree 4 priority 6
   (note - multiplier is 16, default setting is 8)


ArubaOS-Switch# show spanning-tree ?
 bpdu-protection       Show spanning tree BPDU protection status information.
 bpdu-throttle         Displays the configured throttle value.
 config                Show spanning tree configuration information.
 debug-counters        Show spanning tree debug counters information.
 detail                Show spanning tree extended details Port, Bridge, Rx, and Tx
                       report.
 inconsistent-ports    Show information about inconsistent ports blocked by spanning tree
                       protection functions.
 instance              Show the spanning tree instance information.
 mst-config            Show multiple spanning tree region configuration.
 pending               Show spanning tree pending configuration.
 [ethernet] PORT-LIST  Limit the port information printed to the set of the specified
                       ports.
 port-role-change-h... Show the last 10 role change entries on a port in a VLAN/instance.
 pvst-filter           Show spanning tree PVST filter status information.
 pvst-protection       Show spanning tree PVST protection status information.
 root-history          Show spanning tree Root changes history information.
 system-limits         Show system limits for spanning-tree
 topo-change-history   Show spanning tree topology changes history information.
 traps                 Show spanning tree trap information.
 vlan                  Show VLAN information for RPVST.
 <cr>

ArubaOS-Switch# show spanning-tree

 Multiple Spanning Tree (MST) Information

  STP Enabled   : Yes
  Force Version : RSTP-operation
  IST Mapped VLANs : 1-4094
  Switch MAC Address : 009c02-d53980
  Switch Priority    : 8192
  Max Age  : 20
  Max Hops : 20
  Forward Delay : 15

  Topology Change Count  : 29
  Time Since Last Change : 31 mins

  CST Root MAC Address : 009c02-d53980
  CST Root Priority    : 8192
  CST Root Path Cost   : 0
  CST Root Port        : This switch is root

  IST Regional Root MAC Address : 009c02-d53980
  IST Regional Root Priority    : 8192
  IST Regional Root Path Cost   : 0
  IST Remaining Hops            : 20

  Root Guard Ports     :
  Loop Guard Ports     :
  TCN Guard Ports      :
  BPDU Protected Ports :
  BPDU Filtered Ports  :
  PVST Protected Ports :
  PVST Filtered Ports  :
```

```
  Root Inconsistent Ports  :
  Loop Inconsistent Ports  :

                   |           Prio              | Designated    Hello
  Port   Type      | Cost      rity State        | Bridge        Time PtP Edge
  ------ --------- + --------- ---- ------------ + ------------- ---- --- ----
  1      100/1000T | 20000     128  Forwarding   | 009c02-d53980 2    Yes No
  2      100/1000T | Auto      128  Disabled     |               2    Yes No
  3      100/1000T | Auto      128  Disabled     |               2    Yes No
  4      100/1000T | 10000     96   Forwarding   | 009c02-d53980 2    Yes Yes
  5      100/1000T | 20000     128  Forwarding   | 009c02-d53980 2    Yes Yes
  6      100/1000T | Auto      128  Disabled     |               2    Yes No
  7      100/1000T | Auto      128  Disabled     |               2    Yes No
  8      100/1000T | Auto      128  Disabled     |               2    Yes No
  9      100/1000T | Auto      128  Disabled     |               2    Yes No
  10     100/1000T | Auto      128  Disabled     |               2    Yes No
  11     100/1000T | 20000     128  Forwarding   | 009c02-d53980 2    Yes No
  12     100/1000T | Auto      128  Disabled     |               2    Yes No
  13     100/1000T | 20000     128  Forwarding   | 009c02-d53980 2    Yes No
  14     100/1000T | Auto      128  Disabled     |               2    Yes No
  15     100/1000T | 20000     128  Forwarding   | 009c02-d53980 2    Yes Yes
  16     100/1000T | Auto      128  Disabled     |               2    Yes No
  17     100/1000T | Auto      128  Disabled     |               2    Yes No
  18     100/1000T | Auto      128  Disabled     |               2    Yes No
  25               | Auto      128  Disabled     |               2    Yes No
  26               | Auto      128  Disabled     |               2    Yes No
  Trk1             | Auto      64   Disabled     |               2    Yes No
  Trk2             | Auto      64   Disabled     |               2    Yes No
  Trk3             | Auto      64   Disabled     |               2    Yes No
```

Comware5

```
[Comware5]stp ?
  bpdu-protection          Specify BPDU protection
  bridge-diameter          Specify bridge diameter
  config-digest-snooping   Specify configuration digest snooping
  disable                  Disable spanning tree protocol
  enable                   Enable spanning tree protocol
  instance                 Spanning tree instance
  max-hops                 Specify max hops
  mcheck                   Specify mcheck
  mode                     Specify state machine mode
  pathcost-standard        Specify STP port path cost standard
  port-log                 Specify port status logging
  priority                 Specify bridge priority
  region-configuration     Enter MSTP region view
  root                     Specify root switch
  tc-protection            Specify TC protection function
  tc-snooping              Specify TC snooping
  timer                    Specify timer configuration
  timer-factor             Specify aged out time factor
  vlan                     Virtual LAN

[Comware5]stp enable

[Comware5]stp mode ?
  mstp  Multiple spanning tree protocol mode
  pvst  Per-VLAN spanning tree protocol mode
  rstp  Rapid spanning tree protocol mode
```

```
  stp   Spanning tree protocol mode

[Comware5]stp mode rstp

[Comware5]stp priority 12288
   (note - in steps of 4096, default setting is 32768)


[Comware5]interface g1/0/4

[Comware5-GigabitEthernet1/0/4]stp ?
  compliance              MST BPDU Format
  config-digest-snooping  Specify configuration digest snooping
  cost                    Specify port path cost
  disable                 Disable spanning tree protocol on a port
  edged-port              Specify edge port
  enable                  Enable spanning tree protocol on a port
  instance                Spanning tree instance
  loop-protection         Specify loop protection
  mcheck                  Specify mcheck
  no-agreement-check      Specify port ignore agreement information
  point-to-point          Specify point to point link
  port                    Specify port parameter
  root-protection         Specify root protection
  transmit-limit          Specify transmission limit count
  vlan                    Virtual LAN

[Comware5-GigabitEthernet1/0/4]stp edged-port enable

[Comware5-GigabitEthernet1/0/4]stp cost 10000

[Comware5-GigabitEthernet1/0/4]stp port priority 96
   (note - in steps of 16, default setting is 128)


[Comware5]display stp ?
  abnormal-port         Display abnormal ports
  bpdu-statistics       STP BPDU statistics
  brief                 Brief information
  down-port             Port information of protocol down
  history               Root or alternate port history
  instance              Spanning tree instance
  interface             Specify interface
  region-configuration  Region configuration
  root                  Display status and configuration of the root bridge
  slot                  Slot Number
  tc                    Port TC count
  vlan                  Virtual LAN
  |                     Matching output
  <cr>

[Comware5]display stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge         :12288.0023-89d5-a059
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
```

```
CIST Root/ERPC      :8192.009c-02d5-3980 / 20
CIST RegRoot/IRPC   :12288.0023-89d5-a059 / 0
CIST RootPortId     :128.6
BPDU-Protection     :disabled
Bridge Config-
Digest-Snooping     :disabled
TC or TCN received  :0
Time since last TC  :0 days 0h:32m:50s
...
----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :CIST Designated Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=20
 Desg. Bridge/Port   :12288.0023-89d5-a059 / 128.1
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 MST BPDU Format     :Config=auto / Active=802.1s
 Port Config-
 Digest-Snooping     :disabled
 Rapid transition    :true
 Num of Vlans Mapped :1
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 1s RemHop 20
 BPDU Sent           :1026
          TCN: 0, Config: 0, RST: 985, MST: 41
 BPDU Received       :2
          TCN: 0, Config: 0, RST: 0, MST: 2
...
----[Port4(GigabitEthernet1/0/4)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :CIST Designated Port
 Port Priority       :96
 Port Cost(Legacy)   :Config=10000 / Active=10000
 Desg. Bridge/Port   :12288.0023-89d5-a059 / 96.4
 Port Edged          :Config=enabled / Active=enabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 MST BPDU Format     :Config=auto / Active=legacy
 Port Config-
 Digest-Snooping     :disabled
 Rapid transition    :false
 Num of Vlans Mapped :1
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 1s RemHop 20
 BPDU Sent           :1028
          TCN: 0, Config: 0, RST: 988, MST: 40
 BPDU Received       :0
          TCN: 0, Config: 0, RST: 0, MST: 0

----[Port5(GigabitEthernet1/0/5)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :CIST Designated Port
```

```
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=200
 Desg. Bridge/Port   :12288.0023-89d5-a059 / 128.5
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 MST BPDU Format     :Config=auto / Active=legacy
 Port Config-
 Digest-Snooping     :disabled
 Rapid transition    :false
 Num of Vlans Mapped :3
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 1s RemHop 20
 BPDU Sent           :1028
          TCN: 0, Config: 0, RST: 988, MST: 40
 BPDU Received       :0
          TCN: 0, Config: 0, RST: 0, MST: 0

----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :CIST Root Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=20
 Desg. Bridge/Port   :8192.009c-02d5-3980 / 128.11
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 MST BPDU Format     :Config=auto / Active=legacy
 Port Config-
 Digest-Snooping     :disabled
 Num of Vlans Mapped :3
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 0s RemHop 0
 BPDU Sent           :8
          TCN: 0, Config: 0, RST: 0, MST: 8
 BPDU Received       :1034
          TCN: 0, Config: 0, RST: 1034, MST: 0
...


[Comware5]display stp brief
MSTID      Port                          Role  STP State     Protection
   0        GigabitEthernet1/0/1          DESI  FORWARDING    NONE
   0        GigabitEthernet1/0/4          DESI  FORWARDING    NONE
   0        GigabitEthernet1/0/5          DESI  FORWARDING    NONE
   0        GigabitEthernet1/0/6          ROOT  FORWARDING    NONE
```

Comware7

```
[Comware7]stp ?
  bpdu-protection       Specify BPDU protection function
  bridge-diameter       Specify bridge diameter
  global                Specify global parameter
  instance              Specify the spanning tree instance list
  max-hops              Specify max hops
  mode                  Specify state machine mode
```

```
  pathcost-standard     Specify port path cost standard
  port-log              Specify port status logging
  priority              Specify bridge priority
  region-configuration  Enter MSTP region view
  root                  Specify root switch
  tc-protection         Specify TC protection function
  tc-snooping           Specify TC snooping
  timer                 Specify timer configuration
  timer-factor          Specify aged out time factor
  vlan                  Specify the VLAN list

[Comware7]stp mode ?
  mstp  Multiple spanning tree protocol mode
  pvst  Per-Vlan spanning tree mode
  rstp  Rapid spanning tree protocol mode
  stp   Spanning tree protocol mode

[Comware7]stp mode rstp

[Comware7]stp priority 16384
   (note - in steps of 4096, default setting is 32768)


[Comware7]interface g1/0/4

[Comware7-GigabitEthernet1/0/4]stp ?
  compliance              Specify MST BPDU Format
  config-digest-snooping  Specify configuration digest snooping
  cost                    Specify port path cost
  edged-port              Specify edge port
  enable                  Enable STP
  instance                Specify the spanning tree instance list
  loop-protection         Specify loop protection
  mcheck                  Specify mcheck
  no-agreement-check      Specify port ignore agreement information
  point-to-point          Specify point to point link
  port                    Specify port parameter
  role-restriction        Forbid the port to be a root port
  root-protection         Specify root protection
  tc-restriction          Restrict propagation of TC message
  transmit-limit          Specify transmission limit count
  vlan                    Specify the VLAN list

[Comware7-GigabitEthernet1/0/4]stp edged-port

[Comware7-GigabitEthernet1/0/4]stp cost 10000

[Comware7-GigabitEthernet1/0/4]stp port priority 96
   (note - in steps of 16, default setting is 128)


[Comware7]display stp ?
  >                     Redirect it to a file
  >>                    Redirect it to a file in append mode
  abnormal-port         Display abnormal ports
```

```
  bpdu-statistics       BPDU statistics
  brief                 Brief information
  down-port             Port information of protocol down
  history               History of port roles
  instance              Specify the spanning tree instance list
  interface             Specify interface
  region-configuration  Region configuration
  root                  Display status and configuration of the root bridge
  slot                  Specify the slot number
  tc                    Port TC count
  vlan                  Specify the VLAN list
  |                     Matching output
  <cr>

[Comware7]display stp
-------[CIST Global Info][Mode RSTP]-------
 Bridge ID           : 16384.cc3e-5f73-bacb
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
 Root ID/ERPC        : 8192.009c-02d5-3980, 20
 RegRoot ID/IRPC     : 16384.cc3e-5f73-bacb, 0
 RootPort ID         : 128.6
 BPDU-Protection     : Disabled
 Bridge Config-
 Digest-Snooping     : Disabled
 TC or TCN received  : 32
 Time since last TC  : 0 days 0h:37m:8s
...
----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port (Boundary)
 Port ID             : 128.1
 Port cost(Legacy)   : Config=auto, Active=20
 Desg.bridge/port    : 16384.cc3e-5f73-bacb, 128.1
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 TC-Restriction      : Disabled
 Role-Restriction    : Disabled
 Protection type     : Config=none, Active=none
 MST BPDU format     : Config=auto, Active=802.1s
 Port Config-
 Digest-Snooping     : Disabled
 Rapid transition    : True
 Num of VLANs mapped : 1
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 1s RemHops 20
 BPDU sent           : 1528
          TCN: 0, Config: 0, RST: 818, MST: 710
 BPDU received       : 1143
          TCN: 0, Config: 0, RST: 0, MST: 1143
...
----[Port4(GigabitEthernet1/0/4)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port (Boundary)
 Port ID             : 96.4
```

```
 Port cost(Legacy)   : Config=10000, Active=10000
 Desg.bridge/port    : 16384.cc3e-5f73-bacb, 96.4
 Port edged          : Config=enabled, Active=enabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 TC-Restriction      : Disabled
 Role-Restriction    : Disabled
 Protection type     : Config=none, Active=none
 MST BPDU format     : Config=auto, Active=802.1s
 Port Config-
 Digest-Snooping     : Disabled
 Rapid transition    : False
 Num of VLANs mapped : 1
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 1s RemHops 20
 BPDU sent           : 2669
          TCN: 0, Config: 0, RST: 818, MST: 1851
 BPDU received       : 0
          TCN: 0, Config: 0, RST: 0, MST: 0
...
----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Root Port (Boundary)
 Port ID             : 128.6
 Port cost(Legacy)   : Config=auto, Active=20
 Desg.bridge/port    : 8192.009c-02d5-3980, 128.13
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 TC-Restriction      : Disabled
 Role-Restriction    : Disabled
 Protection type     : Config=none, Active=none
 MST BPDU format     : Config=auto, Active=802.1s
 Port Config-
 Digest-Snooping     : Disabled
 Rapid transition    : True
 Num of VLANs mapped : 3
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 0s RemHops 20
 BPDU sent           : 15
          TCN: 0, Config: 0, RST: 0, MST: 15
 BPDU received       : 2664
          TCN: 0, Config: 0, RST: 1480, MST: 1184
...


[Comware7]display stp brief
MST ID   Port                                Role  STP State   Protection
 0        GigabitEthernet1/0/1                DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/4                DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/6                ROOT  FORWARDING  NONE
```

Cisco

not an available feature

Cisco switches operate with PVST+/Rapid PVST+ which is proprietary. MSTP can be configured and automatically enables RSTP, but it is MSTP in its spanning-tree operation. You cannot configure RSTP “only”.

PVST+ is comparable to STP on 802.1Q links (default)
Rapid PVST+ is comparable to RSTP on 802.1Q links

Chapter 22 MSTP

Developed based on the IEEE 802.1s standard, Multiple Spanning Tree Protocol (MSTP) overcomes the limitations of STP and RSTP. In addition to support for rapid network convergence, it allows data flows of different VLANs to be forwarded along separate paths, providing a better load-sharing mechanism for redundant links.

MSTP uses multiple spanning tree instances with separate forwarding topologies. Each instance is composed of one or more VLANs, which significantly improves network link utilization and the speed of reconvergence after a failure in the network's physical topology. However, MSTP requires more configuration overhead and is more susceptible to dropped traffic due to misconfiguration.

This chapter compares the commands you use to configure Multiple Spanning Tree Protocol (MSTP). The four operating systems implement MSTP differently:

- ArubaOS-Switch uses MSTP as the default STP version. MSTP *is not enabled by default*. When MSTP is enabled, all ports are auto-edge-ports.
- Comware5 uses MSTP as the default STP version. MSTP *is not enabled by default*. When MSTP is enabled, all ports are non-edge ports.
- Comware7 uses MSTP as the default STP version, it *is enabled by default,* and all ports are non-edge ports.
- Cisco uses Per-VLAN Spanning Tree Plus (PVST+) as the default STP version and it *is enabled by default*. If you enable MSTP, all ports are non-edge ports.

ArubaOS-Switch	Comware5	Cisco
`ArubaOS-Switch(config)# spanning-tree`	`[Comware5]stp enable`	`Cisco(config)#spanning-tree mode mst`
	`[Comware5]stp region-configuration`	`Cisco(config)#spanning-tree mst configuration`
`ArubaOS-Switch(config)# spanning-tree config-name ArubaOS-Switch-Comware-Cisco`	`[Comware5-mst-region]region-name ArubaOS-Switch-Comware-Cisco`	`Cisco(config-mst)#name ArubaOS-Switch-Comware-Cisco`
`ArubaOS-Switch(config)# spanning-tree config-revision 1`	`[Comware5-mst-region]revision-level 1`	`Cisco(config-mst)#revision 1`
`ArubaOS-Switch(config)# spanning-tree instance 1 vlan 220`	`[Comware5-mst-region]instance 1 vlan 220`	`Cisco(config-mst)# instance 1 vlan 220`
`ArubaOS-Switch(config)# spanning-tree instance 2 vlan 100`	`[Comware5-mst-region]instance 2 vlan 100`	`Cisco(config-mst)# instance 2 vlan 100`
`ArubaOS-Switch(config)# spanning-tree instance 3 vlan 240`	`[Comware5-mst-region]instance 3 vlan 240`	`Cisco(config-mst)# instance 3 vlan 240`
	`[Comware5-mst-region]active region-configuration`	
`ArubaOS-Switch(config)# spanning-tree priority 2`	`[Comware5]stp priority 12288`	`Cisco(config)#spanning-tree mst 0 priority 20480`

ArubaOS-Switch(config)# spanning-tree instance 1 priority 3	[Comware5]stp instance 1 priority 8192	Cisco(config)#spanning-tree mst 1 priority 16384
ArubaOS-Switch(config)# spanning-tree instance 2 priority 4	[Comware5]stp instance 2 priority 20480	Cisco(config)#spanning-tree mst 2 priority 12288
ArubaOS-Switch(config)# spanning-tree instance 3 priority 5	[Comware5]stp instance 3 priority 16384	Cisco(config)#spanning-tree mst 3 priority 8192
	[Comware5]interface g1/0/9	Cisco(config)#interface g1/0/9
ArubaOS-Switch(config)# spanning-tree 9 admin-edge-port	[Comware5-GigabitEthernet1/0/9]stp edged-port enable	Cisco(config-if)#spanning-tree portfast
ArubaOS-Switch(config)# spanning-tree 9 path-cost 10000	[Comware5-GigabitEthernet1/0/9]stp cost 10000	Cisco(config-if)#spanning-tree cost 10000
ArubaOS-Switch(config)# spanning-tree 9 priority 10	[Comware5-GigabitEthernet1/0/9]stp port priority 160	Cisco(config-if)#spanning-tree port-priority 160
ArubaOS-Switch(config)# spanning-tree instance 1 9 path-cost 10000	[Comware5-GigabitEthernet1/0/9]stp instance 1 cost 10000	Cisco(config-if)#spanning-tree mst 1 cost 10000
ArubaOS-Switch(config)# spanning-tree instance 1 9 priority 10	[Comware5-GigabitEthernet1/0/9]stp instance 1 port priority 160	Cisco(config-if)#spanning-tree mst 1 port-priority 160
ArubaOS-Switch# show spanning-tree	[Comware5]display stp	Cisco#show spanning-tree
	[Comware5]display stp brief	
		Cisco#show spanning-tree mst
ArubaOS-Switch# show spanning-tree mst-config	[Comware5]display stp region-configuration	Cisco#show spanning-tree mst configuration
ArubaOS-Switch# show spanning-tree instance ist	[Comware5]display stp instance 0	Cisco#show spanning-tree mst 0
ArubaOS-Switch# show spanning-tree instance 1	[Comware5]display stp instance 1	Cisco#show spanning-tree mst 1
		Cisco#show spanning-tree mst 3
	Comware7	
	[Comware7]stp region-configuration	
	[Comware7-mst-region]region-name ArubaOS-Switch-Comware-Cisco	
	[Comware7-mst-region]revision-level 1	
	[Comware7-mst-region]instance 1 vlan 220	
	[Comware7-mst-region]instance 2 vlan 100	
	[Comware7-mst-region]instance 3 vlan 240	
	[Comware7-mst-region]active region-configuration	
	[Comware7]stp priority 16384	
	[Comware7]stp instance 1 priority 20480	

	[Comware7]stp instance 2 priority 8192	
	[Comware7]stp instance 3 priority 12288	
	[Comware7]interface g1/0/9	
	[Comware7-GigabitEthernet1/0/9]stp edged-port	
	[Comware7-GigabitEthernet1/0/9]stp cost 10000	
	[Comware7-GigabitEthernet1/0/9]stp port priority 160	
	[Comware7-GigabitEthernet1/0/9]stp instance 1 cost 10000	
	[Comware7-GigabitEthernet1/0/9]stp instance 1 port priority 160	
	[Comware7]display stp	
	[Comware7]display stp brief	
	[Comware7]display stp region-configuration	
	[Comware7]display stp instance 0	
	[Comware7]display stp instance 1	
	[Comware7]display stp instance 2	

ArubaOS-Switch

```
ArubaOS-Switch(config)# spanning-tree ?
 bpdu-protection-ti... Set the time for protected ports to be in down state after
                       receiving unauthorized BPDUs.
 bpdu-throttle         Configure BPDU throttling on the device.
 clear-debug-counters  Clear spanning tree debug counters.
 config-name           Set the MST region configuration name (default is switch's MAC
                       address).
 config-revision       Set the MST region configuration revision number (default is 0).
 enable                Enable spanning-tree.
 disable               Disable spanning-tree.
 extend                Enable the extended system ID feature.
 force-version         Set Spanning Tree protocol compatibility mode.
 forward-delay         Set time the switch waits between transitioning from listening to
                       learning and from learning to forwarding states. Not applicable in
                       RPVST mode.
 hello-time            Set time between messages transmission when the switch is root.
                       Not applicable in RPVST mode.
 ignore-pvid-incons... Ignore PVID inconsistencies, allowing Rapid PVST to run on
                       mismatched links.
 instance              Create, delete or configure an MST instance.
 legacy-mode           Set spanning-tree protocol to operate either in 802.1D legacy mode
                       or in 802.1s native mode.
 legacy-path-cost      [Deprecated] Set 802.1D (legacy) or 802.1t (current) default
                       pathcost values.
 log                   Enable event logging for port state transition information.
```

```
 max-hops               Set the max number of hops in a region before the MST BPDU is
                        discarded and the information held for a port is aged (default is
                        20).
 maximum-age            Set maximum age of received STP information before it is
                        discarded. Not applicable in RPVST mode.
 mode                   Specify spanning-tree mode.
 pathcost               Specify a standard to use when calculating the default pathcost.
 pending                Manipulate pending MSTP configuration.
 port                   Configure port specific RPVST parameters for the specified VLANs.
 [ethernet] PORT-LIST   Configure the port-specific parameters of the spanning tree
                        protocol for individual ports.
 priority               Set the device STP priority (the value is in range of 0-61440
                        divided into steps of 4096 that are numbered from 0 to 15, default
                        is step 8). Not applicable in RPVST mode.
 root                   Configure root for STP.
 trap                   Enable/disable STP/MSTP/RPVST traps.
 vlan                   Specify RPVST VLAN specific parameters.
 <cr>

ArubaOS-Switch(config)# spanning-tree

ArubaOS-Switch(config)# spanning-tree config-name ArubaOS-Switch-Comware-Cisco

ArubaOS-Switch(config)# spanning-tree config-revision 1

ArubaOS-Switch(config)# spanning-tree instance 1 vlan 220

ArubaOS-Switch(config)# spanning-tree instance 2 vlan 100

ArubaOS-Switch(config)# spanning-tree instance 3 vlan 240

ArubaOS-Switch(config)# spanning-tree priority 2
   (note - multiplier is 4096, default setting is 8)

ArubaOS-Switch(config)# spanning-tree instance 1 priority 3
   (note - multiplier is 4096, default setting is 8)

ArubaOS-Switch(config)# spanning-tree instance 2 priority 4
   (note - multiplier is 4096, default setting is 8)

ArubaOS-Switch(config)# spanning-tree instance 3 priority 5
   (note - multiplier is 4096, default setting is 8)

ArubaOS-Switch(config)# spanning-tree 9 ?
 admin-edge-port        Set the administrative edge port status.
 auto-edge-port         Set the automatic edge port detection.
 bpdu-filter            Stop a specific port or ports from transmitting BPDUs, receiving
                        BPDUs, and assume a continuous fowarding state.
 bpdu-protection        Disable the specific port or ports if the port(s) receives STP
                        BPDUs.
 hello-time             Set message transmission interval (in sec.) on the port. Not
                        applicable in RPVST mode.
 loop-guard             Set port to guard against the loop and consequently to prevent it
                        from becoming Forwarding Port.
 mcheck                 Force the port to transmit RST BPDUs. Not applicable in RPVST
                        mode.
 path-cost              Set port's path cost value. Not applicable in RPVST mode.
 point-to-point-mac     Set the administrative point-to-point status.
 priority               Set port priority (the value is in range of 0-240 divided into
                        steps of 16 that are numbered from 0 to 15, default is step 8).
                        Not applicable in RPVST mode.
 pvst-filter            Stop a specific port or ports from receiving and retransmitting
                        PVST BPDUs. Not applicable in RPVST mode.
```

```
 pvst-protection       Disable the specific port or ports if the port(s) receives PVST
                       BPDUs. Not applicable in RPVST mode.
 root-guard            Set port to ignore superior BPDUs to prevent it from becoming Root
                       Port.
 tcn-guard             Set port to stop propagating received topology changes
                       notifications and topology changes to other ports.

ArubaOS-Switch(config)# spanning-tree 9 admin-edge-port

ArubaOS-Switch(config)# spanning-tree 9 path-cost 10000

ArubaOS-Switch(config)# spanning-tree 9 priority 10
   (note - multiplier is 16, default setting is 8)


ArubaOS-Switch(config)# spanning-tree instance 1 9 path-cost 10000

ArubaOS-Switch(config)# spanning-tree instance 1 9 priority 10
   (note - multiplier is 16, default setting is 8)


ArubaOS-Switch# show spanning-tree ?
 bpdu-protection       Show spanning tree BPDU protection status information.
 bpdu-throttle         Displays the configured throttle value.
 config                Show spanning tree configuration information.
 debug-counters        Show spanning tree debug counters information.
 detail                Show spanning tree extended details Port, Bridge, Rx, and Tx
                       report.
 inconsistent-ports    Show information about inconsistent ports blocked by spanning tree
                       protection functions.
 instance              Show the spanning tree instance information.
 mst-config            Show multiple spanning tree region configuration.
 pending               Show spanning tree pending configuration.
 [ethernet] PORT-LIST  Limit the port information printed to the set of the specified
                       ports.
 port-role-change-h... Show the last 10 role change entries on a port in a VLAN/instance.
 pvst-filter           Show spanning tree PVST filter status information.
 pvst-protection       Show spanning tree PVST protection status information.
 root-history          Show spanning tree Root changes history information.
 system-limits         Show system limits for spanning-tree
 topo-change-history   Show spanning tree topology changes history information.
 traps                 Show spanning tree trap information.
 vlan                  Show VLAN information for RPVST.
 <cr>

ArubaOS-Switch# show spanning-tree

 Multiple Spanning Tree (MST) Information

  STP Enabled   : Yes
  Force Version : MSTP-operation
  IST Mapped VLANs : 1-99,101-219,221-239,241-4094
  Switch MAC Address : 009c02-d53980
  Switch Priority    : 8192
  Max Age  : 20
  Max Hops : 20
  Forward Delay : 15

  Topology Change Count  : 69
  Time Since Last Change : 6 mins

  CST Root MAC Address : 009c02-d53980
  CST Root Priority    : 8192
```

```
  CST Root Path Cost   : 0
  CST Root Port        : This switch is root

  IST Regional Root MAC Address : 009c02-d53980
  IST Regional Root Priority    : 8192
  IST Regional Root Path Cost   : 0
  IST Remaining Hops            : 20

  Root Guard Ports     :
  Loop Guard Ports     :
  TCN Guard Ports      :
  BPDU Protected Ports :
  BPDU Filtered Ports  :
  PVST Protected Ports :
  PVST Filtered Ports  :

  Root Inconsistent Ports  :
  Loop Inconsistent Ports  :

                   |           Prio               | Designated    Hello
  Port   Type      | Cost      rity State         | Bridge        Time PtP Edge
  ------ --------- + --------- ---- ------------ + ------------- ---- --- ----
  1      100/1000T | 20000     128  Forwarding   | 009c02-d53980 2    Yes No
  2      100/1000T | Auto      128  Disabled     |               2    Yes No
  3      100/1000T | Auto      128  Disabled     |               2    Yes No
  4      100/1000T | 10000     96   Disabled     |               2    Yes Yes
  5      100/1000T | 20000     128  Forwarding   | 009c02-d53980 2    Yes Yes
  6      100/1000T | Auto      128  Disabled     |               2    Yes No
  7      100/1000T | Auto      128  Disabled     |               2    Yes No
  8      100/1000T | Auto      128  Disabled     |               2    Yes No
  9      100/1000T | 10000     160  Forwarding   | 009c02-d53980 2    Yes Yes
  10     100/1000T | Auto      128  Disabled     |               2    Yes No
  11     100/1000T | 20000     128  Forwarding   | 009c02-d53980 2    Yes No
  12     100/1000T | Auto      128  Disabled     |               2    Yes No
  13     100/1000T | 20000     128  Forwarding   | 009c02-d53980 2    Yes No
  14     100/1000T | Auto      128  Disabled     |               2    Yes No
  15     100/1000T | 20000     128  Forwarding   | 009c02-d53980 2    Yes No
  16     100/1000T | Auto      128  Disabled     |               2    Yes No
  17     100/1000T | Auto      128  Disabled     |               2    Yes No
  18     100/1000T | Auto      128  Disabled     |               2    Yes No
  25               | Auto      128  Disabled     |               2    Yes No
  26               | Auto      128  Disabled     |               2    Yes No
  Trk1             | Auto      64   Disabled     |               2    Yes No
  Trk2             | Auto      64   Disabled     |               2    Yes No
  Trk3             | Auto      64   Disabled     |               2    Yes No


ArubaOS-Switch# show spanning-tree mst-config

 MST Configuration Identifier Information

  MST Configuration Name : ArubaOS-Switch-Comware-Cisco
  MST Configuration Revision : 1
  MST Configuration Digest : 0xCEE7F8D6E076E3201F92550CB1D2CB92

  IST Mapped VLANs : 1-99,101-219,221-239,241-4094

  Instance ID Mapped VLANs
  ----------- ------------------------------------------------------------
  1           220
  2           100
  3           240
```

```
ArubaOS-Switch# show spanning-tree instance ist

 IST Instance Information

  Instance ID : 0
  Mapped VLANs : 1-99,101-219,221-239,241-4094
  Switch Priority         : 8192

  Topology Change Count   : 0
  Time Since Last Change  : 9 mins

  Regional Root MAC Address : 009c02-d53980
  Regional Root Priority    : 8192
  Regional Root Path Cost   : 0
  Regional Root Port        : This switch is root
  Remaining Hops            : 20

  Root Inconsistent Ports  :
  Loop Inconsistent Ports  :

                                                            Designated
  Port  Type      Cost      Priority Role       State        Bridge
  ----- --------- --------- -------- ---------- ------------ --------------
  1     100/1000T 20000     128      Designated Forwarding   009c02-d53980
  2     100/1000T Auto      128      Disabled   Disabled
  3     100/1000T Auto      128      Disabled   Disabled
  4     100/1000T Auto      96       Disabled   Disabled
  5     100/1000T 20000     128      Designated Forwarding   009c02-d53980
  6     100/1000T Auto      128      Disabled   Disabled
  7     100/1000T Auto      128      Disabled   Disabled
  8     100/1000T Auto      128      Disabled   Disabled
  9     100/1000T 20000     160      Designated Forwarding   009c02-d53980
  10    100/1000T Auto      128      Disabled   Disabled
  11    100/1000T 20000     128      Designated Forwarding   009c02-d53980
  12    100/1000T Auto      128      Disabled   Disabled
  13    100/1000T 20000     128      Designated Forwarding   009c02-d53980
  14    100/1000T Auto      128      Disabled   Disabled
  15    100/1000T 20000     128      Designated Forwarding   009c02-d53980
  16    100/1000T Auto      128      Disabled   Disabled
  17    100/1000T Auto      128      Disabled   Disabled
  18    100/1000T Auto      128      Disabled   Disabled
  25              Auto      128      Disabled   Disabled
  26              Auto      128      Disabled   Disabled
  Trk1            Auto      64       Disabled   Disabled
  Trk2            Auto      64       Disabled   Disabled
  Trk3            Auto      64       Disabled   Disabled


ArubaOS-Switch# show spanning-tree instance 1

 MST Instance Information

  Instance ID : 1
  Mapped VLANs : 220
  Switch Priority         : 12288

  Topology Change Count   : 62
  Time Since Last Change  : 9 mins

  Regional Root MAC Address : 002389-d5a059
  Regional Root Priority    : 8192
  Regional Root Path Cost   : 20000
```

```
  Regional Root Port        : 11
  Remaining Hops            : 19

  Root Inconsistent Ports  :
  Loop Inconsistent Ports  :

                                                          Designated
  Port  Type      Cost      Priority Role       State        Bridge
  ----- --------- --------- -------- ---------- ------------ --------------
  1     100/1000T 20000     128      Designated Forwarding   009c02-d53980
  2     100/1000T Auto      128      Disabled   Disabled
  3     100/1000T Auto      128      Disabled   Disabled
  4     100/1000T Auto      128      Disabled   Disabled
  5     100/1000T 20000     128      Designated Forwarding   009c02-d53980
  6     100/1000T Auto      128      Disabled   Disabled
  7     100/1000T Auto      128      Disabled   Disabled
  8     100/1000T Auto      128      Disabled   Disabled
  9     100/1000T 20000     160      Designated Forwarding   009c02-d53980
  10    100/1000T Auto      128      Disabled   Disabled
  11    100/1000T 20000     128      Root       Forwarding   002389-d5a059
  12    100/1000T Auto      128      Disabled   Disabled
  13    100/1000T 20000     128      Designated Forwarding   009c02-d53980
  14    100/1000T Auto      128      Disabled   Disabled
  15    100/1000T 20000     128      Designated Forwarding   009c02-d53980
  16    100/1000T Auto      128      Disabled   Disabled
  17    100/1000T Auto      128      Disabled   Disabled
  18    100/1000T Auto      128      Disabled   Disabled
  25              Auto      128      Disabled   Disabled
  26              Auto      128      Disabled   Disabled
  Trk1            Auto      64       Disabled   Disabled
  Trk2            Auto      64       Disabled   Disabled
  Trk3            Auto      64       Disabled   Disabled
```

Comware5

```
[Comware5]stp ?
  bpdu-protection         Specify BPDU protection
  bridge-diameter         Specify bridge diameter
  config-digest-snooping  Specify configuration digest snooping
  disable                 Disable spanning tree protocol
  enable                  Enable spanning tree protocol
  instance                Spanning tree instance
  max-hops                Specify max hops
  mcheck                  Specify mcheck
  mode                    Specify state machine mode
  pathcost-standard       Specify STP port path cost standard
  port-log                Specify port status logging
  priority                Specify bridge priority
  region-configuration    Enter MSTP region view
  root                    Specify root switch
  tc-protection           Specify TC protection function
  tc-snooping             Specify TC snooping
  timer                   Specify timer configuration
  timer-factor            Specify aged out time factor
  vlan                    Virtual LAN

[Comware5]stp enable

[Comware5]stp region-configuration

[Comware5-mst-region]?
Mst-region view commands:
  active          Active region configuration
  cfd             Connectivity fault detection (IEEE 802.1ag)
```

```
  check           Check the reg-configuration under-construction
  display         Display current system information
  instance        Spanning tree instance
  mtracert        Trace route to multicast source
  ping            Ping function
  quit            Exit from current command view
  region-name     Specify region name
  return          Exit to User View
  revision-level  Specify revision level
  save            Save current configuration
  tracert         Trace route function
  undo            Cancel current setting
  vlan-mapping    Vlan mapping

[Comware5-mst-region]region-name ArubaOS-Switch-Comware-Cisco

[Comware5-mst-region]revision-level 1

[Comware5-mst-region]instance 1 vlan 220

[Comware5-mst-region]instance 2 vlan 100

[Comware5-mst-region]instance 3 vlan 240

[Comware5-mst-region]active region-configuration

[Comware5]stp priority 12288
   (note - increments of 4096, default setting is 32768)

[Comware5]stp instance 1 priority 8192
   (note - in steps of 4096, default setting is 32768)

[Comware5]stp instance 2 priority 20480
   (note - in steps of 4096, default setting is 32768)

[Comware5]stp instance 3 priority 16384
   (note - in steps of 4096, default setting is 32768)

[Comware5]interface g1/0/9

[Comware5-GigabitEthernet1/0/9]stp ?
  compliance              MST BPDU Format
  config-digest-snooping  Specify configuration digest snooping
  cost                    Specify port path cost
  disable                 Disable spanning tree protocol on a port
  edged-port              Specify edge port
  enable                  Enable spanning tree protocol on a port
  instance                Spanning tree instance
  loop-protection         Specify loop protection
  mcheck                  Specify mcheck
  no-agreement-check      Specify port ignore agreement information
  point-to-point          Specify point to point link
  port                    Specify port parameter
  root-protection         Specify root protection
  transmit-limit          Specify transmission limit count
  vlan                    Virtual LAN

[Comware5-GigabitEthernet1/0/9]stp edged-port enable

[Comware5-GigabitEthernet1/0/9]stp cost 10000

[Comware5-GigabitEthernet1/0/9]stp port priority 160
   (note - in steps of 16, default setting is 128)
```

```
[Comware5-GigabitEthernet1/0/9]stp instance 1 cost 10000

[Comware5-GigabitEthernet1/0/9]stp instance 1 port priority 160
   (note - in steps of 16, default setting is 128)


[Comware5]display stp ?
  abnormal-port         Display abnormal ports
  bpdu-statistics       STP BPDU statistics
  brief                 Brief information
  down-port             Port information of protocol down
  history               Root or alternate port history
  instance              Spanning tree instance
  interface             Specify interface
  region-configuration  Region configuration
  root                  Display status and configuration of the root bridge
  slot                  Slot Number
  tc                    Port TC count
  vlan                  Virtual LAN
  |                     Matching output
  <cr>

[Comware5]display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :12288.0023-89d5-a059
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :8192.009c-02d5-3980 / 0
CIST RegRoot/IRPC   :8192.009c-02d5-3980 / 20
CIST RootPortId     :128.6
BPDU-Protection     :disabled
Bridge Config-
Digest-Snooping     :disabled
TC or TCN received  :26
Time since last TC  :0 days 0h:11m:55s
...
----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :CIST Root Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=20
 Desg. Bridge/Port   :8192.009c-02d5-3980 / 128.11
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 MST BPDU Format     :Config=auto / Active=802.1s
 Port Config-
 Digest-Snooping     :disabled
 Num of Vlans Mapped :1
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 0s RemHop 20
 BPDU Sent           :2873
          TCN: 0, Config: 0, RST: 0, MST: 2873
 BPDU Received       :2961
          TCN: 0, Config: 0, RST: 0, MST: 2961
...
----[Port9(GigabitEthernet1/0/9)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :CIST Designated Port
 Port Priority       :160
 Port Cost(Legacy)   :Config=10000 / Active=10000
 Desg. Bridge/Port   :12288.0023-89d5-a059 / 160.9
 Port Edged          :Config=enabled / Active=enabled
```

```
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 MST BPDU Format     :Config=auto / Active=legacy
 Port Config-
 Digest-Snooping     :disabled
 Rapid transition    :true
 Num of Vlans Mapped :0
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 0s RemHop 19
 BPDU Sent           :2937
          TCN: 0, Config: 0, RST: 0, MST: 2937
 BPDU Received       :0
          TCN: 0, Config: 0, RST: 0, MST: 0
...
-------[MSTI 1 Global Info]-------
MSTI Bridge ID      :8192.0023-89d5-a059
MSTI RegRoot/IRPC   :8192.0023-89d5-a059 / 0
MSTI RootPortId     :0.0
Master Bridge       :8192.009c-02d5-3980
Cost to Master      :20
TC received         :14
Time since last TC  :0 days 0h:16m:40s

----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=20
 Desg. Bridge/Port   :8192.0023-89d5-a059 / 128.6
 Rapid transition    :true
 Num of Vlans Mapped :1
 Port Times          :RemHops 20

-------[MSTI 2 Global Info]-------
MSTI Bridge ID      :20480.0023-89d5-a059
MSTI RegRoot/IRPC   :8192.cc3e-5f73-bacb / 20020
MSTI RootPortId     :128.6
Master Bridge       :8192.009c-02d5-3980
Cost to Master      :20
TC received         :16
Time since last TC  :0 days 0h:17m:24s

----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=20
 Desg. Bridge/Port   :16384.009c-02d5-3980 / 128.11
 Num of Vlans Mapped :1
 Port Times          :RemHops 19

-------[MSTI 3 Global Info]-------
MSTI Bridge ID      :16384.0023-89d5-a059
MSTI RegRoot/IRPC   :8192.0022-91ab-4380 / 20020
MSTI RootPortId     :128.6
Master Bridge       :8192.009c-02d5-3980
Cost to Master      :20
TC received         :6
Time since last TC  :0 days 0h:19m:30s

 ----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=20
 Desg. Bridge/Port   :20480.009c-02d5-3980 / 128.11
```

```
 Num of Vlans Mapped :1
 Port Times          :RemHops 19


[Comware5]display stp brief
MSTID      Port                          Role  STP State     Protection
   0        GigabitEthernet1/0/1         DESI  FORWARDING    NONE
   0        GigabitEthernet1/0/5         DESI  FORWARDING    NONE
   0        GigabitEthernet1/0/6         ROOT  FORWARDING    NONE
   0        GigabitEthernet1/0/9         DESI  FORWARDING    NONE
   1        GigabitEthernet1/0/5         DESI  FORWARDING    NONE
   1        GigabitEthernet1/0/6         DESI  FORWARDING    NONE
   2        GigabitEthernet1/0/5         DESI  FORWARDING    NONE
   2        GigabitEthernet1/0/6         ROOT  FORWARDING    NONE
   2        GigabitEthernet1/0/9         DESI  FORWARDING    NONE
   3        GigabitEthernet1/0/6         ROOT  FORWARDING    NONE


[Comware5]display stp region-configuration
Oper configuration
   Format selector      :0
   Region name          :ArubaOS-Switch-Comware-Cisco
   Revision level       :1
   Configuration digest :0xcee7f8d6e076e3201f92550cb1d2cb92

   Instance   Vlans Mapped
      0       1 to 99, 101 to 219, 221 to 239, 241 to 4094
      1       220
      2       100
      3       240


[Comware5]display stp instance 0
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :12288.0023-89d5-a059
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :8192.009c-02d5-3980 / 0
CIST RegRoot/IRPC   :8192.009c-02d5-3980 / 20
CIST RootPortId     :128.6
BPDU-Protection     :disabled
Bridge Config-
Digest-Snooping     :disabled
TC or TCN received  :26
Time since last TC  :0 days 0h:24m:21s
...
----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :CIST Root Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=20
 Desg. Bridge/Port   :8192.009c-02d5-3980 / 128.11
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 MST BPDU Format     :Config=auto / Active=802.1s
 Port Config-
 Digest-Snooping     :disabled
 Num of Vlans Mapped :1
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 0s RemHop 20
 BPDU Sent           :3253
          TCN: 0, Config: 0, RST: 0, MST: 3253
 BPDU Received       :3344
```

```
          TCN: 0, Config: 0, RST: 0, MST: 3344
...
----[Port9(GigabitEthernet1/0/9)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :CIST Designated Port
 Port Priority       :160
 Port Cost(Legacy)   :Config=10000 / Active=10000
 Desg. Bridge/Port   :12288.0023-89d5-a059 / 160.9
 Port Edged          :Config=enabled / Active=enabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 MST BPDU Format     :Config=auto / Active=legacy
 Port Config-
 Digest-Snooping     :disabled
 Rapid transition    :true
 Num of Vlans Mapped :0
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 0s RemHop 19
 BPDU Sent           :3327
          TCN: 0, Config: 0, RST: 0, MST: 3327
 BPDU Received       :0
          TCN: 0, Config: 0, RST: 0, MST: 0
...


[Comware5]display stp instance 1
-------[MSTI 1 Global Info]-------
MSTI Bridge ID      :8192.0023-89d5-a059
MSTI RegRoot/IRPC   :8192.0023-89d5-a059 / 0
MSTI RootPortId     :0.0
Master Bridge       :8192.009c-02d5-3980
Cost to Master      :20
TC received         :14
Time since last TC  :0 days 0h:26m:4s

 ----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=20
 Desg. Bridge/Port   :8192.0023-89d5-a059 / 128.6
 Rapid transition    :true
 Num of Vlans Mapped :1
 Port Times          :RemHops 20
```

Comware7

```
[Comware7]stp ?
  bpdu-protection       Specify BPDU protection function
  bridge-diameter       Specify bridge diameter
  global                Specify global parameter
  instance              Specify the spanning tree instance list
  max-hops              Specify max hops
  mode                  Specify state machine mode
  pathcost-standard     Specify port path cost standard
  port-log              Specify port status logging
  priority              Specify bridge priority
  region-configuration  Enter MSTP region view
  root                  Specify root switch
  tc-protection         Specify TC protection function
  tc-snooping           Specify TC snooping
  timer                 Specify timer configuration
  timer-factor          Specify aged out time factor
  vlan                  Specify the VLAN list
```

```
[Comware7]stp region-configuration

[Comware7-mst-region]?
Mst-region view commands:
  active              Active region configuration
  cfd                 Connectivity Fault Detection (CFD) module
  check               Check the reg-configuration under-construction
  diagnostic-logfile  Diagnostic log file configuration
  display             Display current system information
  instance            Specify the spanning tree instance list
  logfile             Log file configuration
  monitor             System monitor
  ping                Ping function
  quit                Exit from current command view
  region-name         Specify region name
  return              Exit to User View
  revision-level      Specify revision level
  save                Save current configuration
  security-logfile    Security log file configuration
  tracert             Tracert function
  undo                Cancel current setting
  vlan-mapping        VLAN mapping

[Comware7-mst-region]region-name ArubaOS-Switch-Comware-Cisco

[Comware7-mst-region]revision-level 1

[Comware7-mst-region]instance 1 vlan 220

[Comware7-mst-region]instance 2 vlan 100

[Comware7-mst-region]instance 3 vlan 240

[Comware7-mst-region]active region-configuration

[Comware7]stp priority 16384
   (note - increments of 4096, default setting is 32768)

[Comware7]stp instance 1 priority 20480
   (note – in steps of 4096, default setting is 32768)

[Comware7]stp instance 2 priority 8192
   (note – in steps of 4096, default setting is 32768)

[Comware7]stp instance 3 priority 12288
   (note – in steps of 4096, default setting is 32768)

[Comware7]interface g1/0/9

[Comware7-GigabitEthernet1/0/9]stp ?
  compliance              Specify MST BPDU Format
  config-digest-snooping  Specify configuration digest snooping
  cost                    Specify port path cost
  edged-port              Specify edge port
  enable                  Enable STP
  instance                Specify the spanning tree instance list
  loop-protection         Specify loop protection
  mcheck                  Specify mcheck
  no-agreement-check      Specify port ignore agreement information
  point-to-point          Specify point to point link
  port                    Specify port parameter
  role-restriction        Forbid the port to be a root port
  root-protection         Specify root protection
```

```
  tc-restriction          Restrict propagation of TC message
  transmit-limit          Specify transmission limit count
  vlan                    Specify the VLAN list

[Comware7-GigabitEthernet1/0/9]stp edged-port

[Comware7-GigabitEthernet1/0/9]stp cost 10000

[Comware7-GigabitEthernet1/0/9]stp port priority 160
   (note - in steps of 16, default setting is 128)

[Comware7-GigabitEthernet1/0/9]stp instance 1 cost 10000

[Comware7-GigabitEthernet1/0/9]stp instance 1 port priority 160
   (note - in steps of 16, default setting is 128)


[Comware7]display stp ?
  >                     Redirect it to a file
  >>                    Redirect it to a file in append mode
  abnormal-port         Display abnormal ports
  bpdu-statistics       BPDU statistics
  brief                 Brief information
  down-port             Port information of protocol down
  history               History of port roles
  instance              Specify the spanning tree instance list
  interface             Specify interface
  region-configuration  Region configuration
  root                  Display status and configuration of the root bridge
  slot                  Specify the slot number
  tc                    Port TC count
  vlan                  Specify the VLAN list
  |                     Matching output
  <cr>

[Comware7]display stp
-------[CIST Global Info][Mode MSTP]-------
 Bridge ID           : 16384.cc3e-5f73-bacb
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
 Root ID/ERPC        : 8192.009c-02d5-3980, 0
 RegRoot ID/IRPC     : 8192.009c-02d5-3980, 20
 RootPort ID         : 128.6
 BPDU-Protection     : Disabled
 Bridge Config-
 Digest-Snooping     : Disabled
 TC or TCN received  : 68
 Time since last TC  : 0 days 0h:29m:41s
...
----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Root Port
 Port ID             : 128.6
 Port cost(Legacy)   : Config=auto, Active=20
 Desg.bridge/port    : 8192.009c-02d5-3980, 128.13
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 TC-Restriction      : Disabled
 Role-Restriction    : Disabled
 Protection type     : Config=none, Active=none
 MST BPDU format     : Config=auto, Active=802.1s
 Port Config-
 Digest-Snooping     : Disabled
```

```
 Rapid transition    : True
 Num of VLANs mapped : 1
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 0s RemHops 20
 BPDU sent           : 2745
          TCN: 0, Config: 0, RST: 3, MST: 2742
 BPDU received       : 5273
          TCN: 0, Config: 0, RST: 1426, MST: 3847
...
----[Port9(GigabitEthernet1/0/9)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port
 Port ID             : 160.9
 Port cost(Legacy)   : Config=10000, Active=10000
 Desg.bridge/port    : 16384.cc3e-5f73-bacb, 160.9
 Port edged          : Config=enabled, Active=enabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 TC-Restriction      : Disabled
 Role-Restriction    : Disabled
 Protection type     : Config=none, Active=none
 MST BPDU format     : Config=auto, Active=802.1s
 Port Config-
 Digest-Snooping     : Disabled
 Rapid transition    : True
 Num of VLANs mapped : 0
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 0s RemHops 19
 BPDU sent           : 5604
          TCN: 0, Config: 0, RST: 876, MST: 4728
 BPDU received       : 0
          TCN: 0, Config: 0, RST: 0, MST: 0
...
-------[MSTI 1 Global Info]-------
 Bridge ID           : 20480.cc3e-5f73-bacb
 RegRoot ID/IRPC     : 8192.0023-89d5-a059, 20020
 RootPort ID         : 128.6
 Master bridge       : 8192.009c-02d5-3980
 Cost to master      : 20
 TC received         : 0

----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Root Port
 Port ID             : 128.6
 Port cost(Legacy)   : Config=auto, Active=20
 Desg.bridge/port    : 12288.009c-02d5-3980, 128.13
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Num of VLANs mapped : 1
 Port times          : RemHops 19

-------[MSTI 2 Global Info]-------
 Bridge ID           : 8192.cc3e-5f73-bacb
 RegRoot ID/IRPC     : 8192.cc3e-5f73-bacb, 0
 RootPort ID         : 0.0
 Master bridge       : 8192.009c-02d5-3980
 Cost to master      : 20
 TC received         : 0

----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port
 Port ID             : 128.6
 Port cost(Legacy)   : Config=auto, Active=20
```

```
 Desg.bridge/port    : 8192.cc3e-5f73-bacb, 128.6
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Num of VLANs mapped : 1
 Port times          : RemHops 20

----[Port9(GigabitEthernet1/0/9)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port
 Port ID             : 128.9
 Port cost(Legacy)   : Config=auto, Active=200
 Desg.bridge/port    : 8192.cc3e-5f73-bacb, 128.9
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Num of VLANs mapped : 1
 Port times          : RemHops 20

-------[MSTI 3 Global Info]-------
 Bridge ID           : 12288.cc3e-5f73-bacb
 RegRoot ID/IRPC     : 8192.0022-91ab-4380, 20020
 RootPort ID         : 128.6
 Master bridge       : 8192.009c-02d5-3980
 Cost to master      : 20
 TC received         : 0

----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Root Port
 Port ID             : 128.6
 Port cost(Legacy)   : Config=auto, Active=20
 Desg.bridge/port    : 20480.009c-02d5-3980, 128.13
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Num of VLANs mapped : 1
 Port times          : RemHops 19


[Comware7]display stp brief
MST ID   Port                                Role  STP State   Protection
 0        GigabitEthernet1/0/1                DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/6                ROOT  FORWARDING  NONE
 0        GigabitEthernet1/0/9                DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/6                ROOT  FORWARDING  NONE
 2        GigabitEthernet1/0/6                DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/9                DESI  FORWARDING  NONE
 3        GigabitEthernet1/0/6                ROOT  FORWARDING  NONE


[Comware7]display stp region-configuration
Oper Configuration
   Format selector      : 0
   Region name          : ArubaOS-Switch-Comware-Cisco
   Revision level       : 1
   Configuration digest : 0xcee7f8d6e076e3201f92550cb1d2cb92

   Instance  VLANs Mapped
   0         1 to 99, 101 to 219, 221 to 239, 241 to 4094
   1         220
   2         100
   3         240


[Comware7]display stp instance 0
```

```
-------[CIST Global Info][Mode MSTP]-------
 Bridge ID           : 16384.cc3e-5f73-bacb
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
 Root ID/ERPC        : 8192.009c-02d5-3980, 0
 RegRoot ID/IRPC     : 8192.009c-02d5-3980, 20
 RootPort ID         : 128.6
 BPDU-Protection     : Disabled
 Bridge Config-
 Digest-Snooping     : Disabled
 TC or TCN received  : 68
 Time since last TC  : 0 days 0h:34m:59s
...
----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Root Port
 Port ID             : 128.6
 Port cost(Legacy)   : Config=auto, Active=20
 Desg.bridge/port    : 8192.009c-02d5-3980, 128.13
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 TC-Restriction      : Disabled
 Role-Restriction    : Disabled
 Protection type     : Config=none, Active=none
 MST BPDU format     : Config=auto, Active=802.1s
 Port Config-
 Digest-Snooping     : Disabled
 Rapid transition    : True
 Num of VLANs mapped : 1
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 0s RemHops 20
 BPDU sent           : 2904
          TCN: 0, Config: 0, RST: 3, MST: 2901
 BPDU received       : 5431
          TCN: 0, Config: 0, RST: 1426, MST: 4005
...
----[Port9(GigabitEthernet1/0/9)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port
 Port ID             : 160.9
 Port cost(Legacy)   : Config=10000, Active=10000
 Desg.bridge/port    : 16384.cc3e-5f73-bacb, 160.9
 Port edged          : Config=enabled, Active=enabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 TC-Restriction      : Disabled
 Role-Restriction    : Disabled
 Protection type     : Config=none, Active=none
 MST BPDU format     : Config=auto, Active=802.1s
 Port Config-
 Digest-Snooping     : Disabled
 Rapid transition    : True
 Num of VLANs mapped : 0
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 0s RemHops 19
 BPDU sent           : 5763
          TCN: 0, Config: 0, RST: 876, MST: 4887
 BPDU received       : 0
          TCN: 0, Config: 0, RST: 0, MST: 0
...


[Comware7]display stp instance 1
-------[MSTI 1 Global Info]-------
 Bridge ID           : 20480.cc3e-5f73-bacb
```

```
 RegRoot ID/IRPC     : 8192.0023-89d5-a059, 20020
 RootPort ID         : 128.6
 Master bridge       : 8192.009c-02d5-3980
 Cost to master      : 20
 TC received         : 0

----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Root Port
 Port ID             : 128.6
 Port cost(Legacy)   : Config=auto, Active=20
 Desg.bridge/port    : 12288.009c-02d5-3980, 128.13
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Num of VLANs mapped : 1
 Port times          : RemHops 19


[Comware7]display stp instance 2
-------[MSTI 2 Global Info]-------
 Bridge ID           : 8192.cc3e-5f73-bacb
 RegRoot ID/IRPC     : 8192.cc3e-5f73-bacb, 0
 RootPort ID         : 0.0
 Master bridge       : 8192.009c-02d5-3980
 Cost to master      : 20
 TC received         : 0

----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port
 Port ID             : 128.6
 Port cost(Legacy)   : Config=auto, Active=20
 Desg.bridge/port    : 8192.cc3e-5f73-bacb, 128.6
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Num of VLANs mapped : 1
 Port times          : RemHops 20

----[Port9(GigabitEthernet1/0/9)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port
 Port ID             : 128.9
 Port cost(Legacy)   : Config=auto, Active=200
 Desg.bridge/port    : 8192.cc3e-5f73-bacb, 128.9
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Num of VLANs mapped : 1
 Port times          : RemHops 20
```

Cisco

```
Cisco(config)#spanning-tree ?
  backbonefast  Enable BackboneFast Feature
  etherchannel  Spanning tree etherchannel specific configuration
  extend        Spanning Tree 802.1t extensions
  logging       Enable Spanning tree logging
  loopguard     Spanning tree loopguard options
  mode          Spanning tree operating mode
  mst           Multiple spanning tree configuration
  pathcost      Spanning tree pathcost options
  portfast      Spanning tree portfast options
  transmit      STP transmit parameters
  uplinkfast    Enable UplinkFast Feature
  vlan          VLAN Switch Spanning Tree
```

```
Cisco(config)#spanning-tree mode ?
  mst         Multiple spanning tree mode
  pvst        Per-Vlan spanning tree mode
  rapid-pvst  Per-Vlan rapid spanning tree mode

Cisco(config)#spanning-tree mode mst

Cisco(config)#spanning-tree mst configuration

Cisco(config-mst)#?
  abort         Exit region configuration mode, aborting changes
  exit          Exit region configuration mode, applying changes
  instance      Map vlans to an MST instance
  name          Set configuration name
  no            Negate a command or set its defaults
  private-vlan  Set private-vlan synchronization
  revision      Set configuration revision number
  show          Display region configurations

Cisco(config-mst)#name ArubaOS-Switch-Comware-Cisco

Cisco(config-mst)#revision 1

Cisco(config-mst)# instance 1 vlan 220

Cisco(config-mst)# instance 2 vlan 100

Cisco(config-mst)# instance 3 vlan 240

Cisco(config)#spanning-tree mst 0 priority 20480
   (note - increments of 4096, default setting is 32768)

Cisco(config)#spanning-tree mst 1 priority 16384
   (note - increments of 4096, default setting is 32768)

Cisco(config)#spanning-tree mst 2 priority 12288
   (note - increments of 4096, default setting is 32768)

Cisco(config)#spanning-tree mst 3 priority 8192
   (note - increments of 4096, default setting is 32768)


Cisco(config)#interface g1/0/9

Cisco(config-if)#spanning-tree ?
  bpdufilter     Don't send or receive BPDUs on this interface
  bpduguard      Don't accept BPDUs on this interface
  cost           Change an interface's spanning tree port path cost
  guard          Change an interface's spanning tree guard mode
  link-type      Specify a link type for spanning tree protocol use
  mst            Multiple spanning tree
  port-priority  Change an interface's spanning tree port priority
  portfast       Enable an interface to move directly to forwarding on link up
  stack-port     Enable stack port
  vlan           VLAN Switch Spanning Tree

Cisco(config-if)#spanning-tree portfast

Cisco(config-if)#spanning-tree cost 10000

Cisco(config-if)#spanning-tree port-priority 160
   (note - increments of 16, default setting is 128)
```

```
Cisco(config-if)#spanning-tree mst 1 cost 10000

Cisco(config-if)#spanning-tree mst 1 port-priority 160
   (note - increments of 16, default setting is 128)


Cisco#show spanning-tree ?
  active             Report on active interfaces only
  backbonefast       Show spanning tree backbonefast status
  blockedports       Show blocked ports
  bridge             Status and configuration of this bridge
  detail             Detailed information
  inconsistentports  Show inconsistent ports
  interface          Spanning Tree interface status and configuration
  mst                Multiple spanning trees
  pathcost           Show Spanning pathcost options
  root               Status and configuration of the root bridge
  summary            Summary of port states
  uplinkfast         Show spanning tree uplinkfast status
  vlan               VLAN Switch Spanning Trees
  |                  Output modifiers
  <cr>

Cisco#show spanning-tree

MST0
  Spanning tree enabled protocol mstp
  Root ID    Priority    8192
             Address     009c.02d5.3980
             Cost        0
             Port        6 (GigabitEthernet1/0/6)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    20480  (priority 20480 sys-id-ext 0)
             Address     0022.91ab.4380
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Desg FWD 20000     128.1    P2p
Gi1/0/6             Root FWD 20000     128.6    P2p
Gi1/0/9             Desg FWD 10000     160.9    P2p Edge



MST1
  Spanning tree enabled protocol mstp
  Root ID    Priority    8193
             Address     0023.89d5.a059
             Cost        40000
             Port        6 (GigabitEthernet1/0/6)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    16385  (priority 16384 sys-id-ext 1)
             Address     0022.91ab.4380
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/6             Root FWD 20000     128.6    P2p
```

```
MST2
  Spanning tree enabled protocol mstp
  Root ID    Priority    8194
             Address     cc3e.5f73.bacb
             Cost        40000
             Port        6 (GigabitEthernet1/0/6)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    12290  (priority 12288 sys-id-ext 2)
             Address     0022.91ab.4380
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/6             Root FWD 20000     128.6    P2p
Gi1/0/9             Desg FWD 10000     160.9    P2p Edge



MST3
  Spanning tree enabled protocol mstp
  Root ID    Priority    8195
             Address     0022.91ab.4380
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    8195   (priority 8192 sys-id-ext 3)
             Address     0022.91ab.4380
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/6             Desg FWD 20000     128.6    P2p


Cisco#show spanning-tree mst

##### MST0    vlans mapped:   1-99,101-219,221-239,241-4094
Bridge        address 0022.91ab.4380  priority      20480 (20480 sysid 0)
Root          address 009c.02d5.3980  priority      8192  (8192 sysid 0)
              port    Gi1/0/6         path cost     0
Regional Root address 009c.02d5.3980  priority      8192  (8192 sysid 0)
                                      internal cost 20000     rem hops 19
Operational   hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured    hello time 2 , forward delay 15, max age 20, max hops    20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1          Desg FWD 20000     128.1    P2p
Gi1/0/6          Root FWD 20000     128.6    P2p
Gi1/0/9          Desg FWD 10000     160.9    P2p Edge

##### MST1    vlans mapped:   220
Bridge        address 0022.91ab.4380  priority      16385 (16384 sysid 1)
Root          address 0023.89d5.a059  priority      8193  (8192 sysid 1)
              port    Gi1/0/6         cost          40000     rem hops 18

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/6          Root FWD 20000     128.6    P2p

##### MST2    vlans mapped:   100
```

```
Bridge        address 0022.91ab.4380  priority      12290 (12288 sysid 2)
Root          address cc3e.5f73.bacb  priority      8194  (8192 sysid 2)
              port    Gi1/0/6         cost          40000     rem hops 18

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/6          Root FWD 20000     128.6    P2p
Gi1/0/9          Desg FWD 10000     160.9    P2p Edge

##### MST3    vlans mapped:   240
Bridge        address 0022.91ab.4380  priority      8195  (8192 sysid 3)
Root          this switch for MST3

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/6          Desg FWD 20000     128.6    P2p


Cisco#show spanning-tree mst configuration
Name      [ArubaOS-Switch-Comware-Cisco]
Revision  1     Instances configured 4

Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-99,101-219,221-239,241-4094
1         220
2         100
3         240
-------------------------------------------------------------------------------


Cisco#show spanning-tree mst 0

##### MST0    vlans mapped:   1-99,101-219,221-239,241-4094
Bridge        address 0022.91ab.4380  priority      20480 (20480 sysid 0)
Root          address 009c.02d5.3980  priority      8192  (8192 sysid 0)
              port    Gi1/0/6         path cost     0
Regional Root address 009c.02d5.3980  priority      8192  (8192 sysid 0)
                                      internal cost 20000     rem hops 19
Operational   hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured    hello time 2 , forward delay 15, max age 20, max hops    20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1          Desg FWD 20000     128.1    P2p
Gi1/0/6          Root FWD 20000     128.6    P2p
Gi1/0/9          Desg FWD 10000     160.9    P2p Edge


Cisco#show spanning-tree mst 1

##### MST1    vlans mapped:   220
Bridge        address 0022.91ab.4380  priority      16385 (16384 sysid 1)
Root          address 0023.89d5.a059  priority      8193  (8192 sysid 1)
              port    Gi1/0/6         cost          40000     rem hops 18

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/6          Root FWD 20000     128.6    P2p


Cisco#show spanning-tree mst 3
```

```
##### MST3    vlans mapped:   240
Bridge        address 0022.91ab.4380  priority      8195  (8192 sysid 3)
Root          this switch for MST3

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/6          Desg FWD 20000     128.6    P2p
```

Chapter 23 PVST/PVST+/RPVST/RPVST+

Cisco implements Per-VLAN Spanning Tree Plus (PVST+), which is based on the IEEE 802.1D standard (Spanning Tree Protocol [STP]) and additional proprietary extensions, or Rapid Per-VLAN Spanning Tree Plus (RPVST+), which is based on the IEEE 802.1w standard (Rapid STP [RSTP]) and additional proprietary extensions. As noted in chapter 19, Cisco also implements MSTP.

Unlike STP and RSTP, whose bridges in a LAN must forward their VLAN packets in the same spanning tree, PVST allows each VLAN to build a separate spanning tree.

RPVST+ is a proprietary spanning tree implementation that extends RSTP (802.1w) to run a separate spanning tree for each VLAN on the switch, and ensures that only one active, loop-free path exists between any two nodes on a given VLAN.

ArubaOS-Switch has RPVST+ capability and Comware has PVST+ capability.

This chapter compares the commands required to configure RPVST+/PVST+ as appropriate for each platform.

The four operating systems default spanning-tree configuration state is as follows:

- ArubaOS-Switch uses MSTP as the default STP version and *is not enabled by default*.
- Comware5 uses MSTP as the default STP version and *is not enabled by default*.
- Comware7 uses MSTP as the default STP version and *is enabled by default*.
- Cisco uses Per-VLAN Spanning Tree Plus (PVST+) as the default STP version and *is enabled by default*.

ArubaOS-Switch	Comware5	Cisco
`ArubaOS-Switch(config)# spanning-tree mode rapid-pvst`	`[Comware5]stp mode pvst`	`Cisco(config)#spanning-tree mode rapid-pvst` (note – this is the default spanning-tree mode, command is shown for refernece)
`ArubaOS-Switch(config)# spanning-tree vlan 1 priority 2`	`[Comware5]stp vlan 1 priority 12288`	`Cisco(config)#spanning-tree vlan 1 priority 20480`
`ArubaOS-Switch(config)# spanning-tree vlan 220 priority 3`	`[Comware5]stp vlan 220 priority 8192`	`Cisco(config)#spanning-tree vlan 220 priority 16384`
`ArubaOS-Switch(config)# spanning-tree vlan 100 priority 4`	`[Comware5]stp vlan 100 priority 20480`	`Cisco(config)#spanning-tree vlan 100 priority 12288`
`ArubaOS-Switch(config)# spanning-tree vlan 240 priority 5`	`[Comware5]stp vlan 240 priority 16384`	`Cisco(config)#spanning-tree vlan 240 priority 8192`
`ArubaOS-Switch(config)# spanning-tree`	`[Comware5]stp enable`	
`ArubaOS-Switch# show spanning-tree`	`[Comware5]display stp root`	`Cisco#show spanning-tree root`

	[Comware5]display stp	Cisco#show spanning-tree summary
	Comware7	
	[Comware7]stp mode pvst	
	[Comware7]stp vlan 1 priority 16384	
	[Comware7]stp vlan 220 priority 20480	
	[Comware7]stp vlan 100 priority 8192	
	[Comware7]stp vlan 240 priority 12288	
	[Comware7]stp global enable	
	[Comware7]display stp root [Comware7]display stp	

ArubaOS-Switch

```
ArubaOS-Switch(config)# spanning-tree mode
 mstp                   Specify spanning tree to run in MSTP mode.
 rapid-pvst             Specify spanning tree to run in Rapid PVST mode.

ArubaOS-Switch(config)# spanning-tree mode rapid-pvst


ArubaOS-Switch(config)# spanning-tree ?
bpdu-protection-ti... Set the time for protected ports to be in down state after
                       receiving unauthorized BPDUs.
 bpdu-throttle         Configure BPDU throttling on the device.
 clear-debug-counters  Clear spanning tree debug counters.
 config-name           Set the MST region configuration name (default is switch's MAC
                       address).
 config-revision       Set the MST region configuration revision number (default is 0).
 enable                Enable spanning-tree.
 disable               Disable spanning-tree.
 extend                Enable the extended system ID feature.
 force-version         Set Spanning Tree protocol compatibility mode.
 forward-delay         Set time the switch waits between transitioning from listening to
                       learning and from learning to forwarding states. Not applicable in
                       RPVST mode.
 hello-time            Set time between messages transmission when the switch is root.
                       Not applicable in RPVST mode.
 ignore-pvid-incons... Ignore PVID inconsistencies, allowing Rapid PVST to run on
                       mismatched links.
 instance              Create, delete or configure an MST instance.
 legacy-mode           Set spanning-tree protocol to operate either in 802.1D legacy mode
                       or in 802.1s native mode.
 legacy-path-cost      [Deprecated] Set 802.1D (legacy) or 802.1t (current) default
                       pathcost values.
 log                   Enable event logging for port state transition information.
 max-hops              Set the max number of hops in a region before the MST BPDU is
                       discarded and the information held for a port is aged (default is
                       20).
 maximum-age           Set maximum age of received STP information before it is
                       discarded. Not applicable in RPVST mode.
 mode                  Specify spanning-tree mode.
```

```
 pathcost               Specify a standard to use when calculating the default pathcost.
 pending                Manipulate pending MSTP configuration.
 port                   Configure port specific RPVST parameters for the specified VLANs.
 [ethernet] PORT-LIST   Configure the port-specific parameters of the spanning tree
                        protocol for individual ports.
 priority               Set the device STP priority (the value is in range of 0-61440
                        divided into steps of 4096 that are numbered from 0 to 15, default
                        is step 8). Not applicable in RPVST mode.
 root                   Configure root for STP.
 trap                   Enable/disable STP/MSTP/RPVST traps.
 vlan                   Specify RPVST VLAN specific parameters.
 <cr>

ArubaOS-Switch(config)# spanning-tree vlan ?
 [vlan]VLAN-ID-LIST    Enter a list of VLAN identifiers or one VLAN identifier.

ArubaOS-Switch(config)# spanning-tree vlan 1 ?
enable                 Enable RPVST on the specified VLANs. This is default.
 disable                Disable RPVST on the specified VLANs.
 forward-delay          Set time the switch waits between transitioning from listening to
                        learning and from learning to forwarding states for specified
                        VLANs.
 hello-time             Set time between messages transmission when the switch is root for
                        specified VLANs.
 maximum-age            Set maximum age of received STP information before it is discarded
                        for specified VLANs.
 priority               Set the device STP priority for the specified VLANs (the value is
                        in range of 0-61440 divided into steps of 4096 that are numbered
                        from 0 to 15, default is step 8).
 root                   Explictly configure the switch as the primary or secondary root
                        bridge for the specified VLANs.

ArubaOS-Switch(config)# spanning-tree vlan 1 priority 2
   (note - multiplier is 4096, default setting is 8)

ArubaOS-Switch(config)# spanning-tree vlan 220 priority 3

ArubaOS-Switch(config)# spanning-tree vlan 100 priority 4

ArubaOS-Switch(config)# spanning-tree vlan 240 priority 5


ArubaOS-Switch(config)# spanning-tree


ArubaOS-Switch# show spanning-tree ?
bpdu-protection        Show spanning tree BPDU protection status information.
 bpdu-throttle          Displays the configured throttle value.
 config                 Show spanning tree configuration information.
 debug-counters         Show spanning tree debug counters information.
 detail                 Show spanning tree extended details Port, Bridge, Rx, and Tx
                        report.
 inconsistent-ports     Show information about inconsistent ports blocked by spanning tree
                        protection functions.
 instance               Show the spanning tree instance information.
 mst-config             Show multiple spanning tree region configuration.
 pending                Show spanning tree pending configuration.
 [ethernet] PORT-LIST   Limit the port information printed to the set of the specified
                        ports.
 port-role-change-h... Show the last 10 role change entries on a port in a VLAN/instance.
 pvst-filter            Show spanning tree PVST filter status information.
 pvst-protection        Show spanning tree PVST protection status information.
 root-history           Show spanning tree Root changes history information.
```

```
 system-limits          Show system limits for spanning-tree
 topo-change-history    Show spanning tree topology changes history information.
 traps                  Show spanning tree trap information.
 vlan                   Show VLAN information for RPVST.
 <cr>

ArubaOS-Switch# show spanning-tree

 Spanning Tree Information

  STP Enabled          [No] : Yes
  Mode                      : RPVST
  Extended System ID        : Enabled
  Ignore PVID Inconsistency : Disabled
  RPVST Enabled VLANs       : 1,100,220,230,240


  Switch MAC Address        : 009c02-d53980
  Root Guard Ports          :
  Loop Guard Ports          :
  TCN Guard Ports           :
  BPDU Protected Ports      :
  BPDU Filtered Ports       :
  Auto Edge Ports           : 1-18,25-26,Trk1-Trk3
  Admin Edge Ports          : 9

  VLAN  Root Mac        Root       Root       Root                 Hello
  ID    Address         Priority   Path-Cost  Port                 Time(sec)
  ----- --------------- ---------- ---------- -------------------- ---------
  1     009c02-d53980   8192       0          This switch is root  2
  100   cc3e5f-73bacb   8192       20,000     13                   2
  220   002389-d5a059   8192       20,000     11                   2
  230   002291-ab4380   32,768     20,000     15                   2
  240   002291-ab4380   8192       20,000     15                   2
```

Comware5

```
[Comware5]stp ?
  bpdu-protection          Specify BPDU protection
  bridge-diameter          Specify bridge diameter
  config-digest-snooping   Specify configuration digest snooping
  disable                  Disable spanning tree protocol
  enable                   Enable spanning tree protocol
  instance                 Spanning tree instance
  max-hops                 Specify max hops
  mcheck                   Specify mcheck
  mode                     Specify state machine mode
  pathcost-standard        Specify STP port path cost standard
  port-log                 Specify port status logging
  priority                 Specify bridge priority
  region-configuration     Enter MSTP region view
  root                     Specify root switch
  tc-protection            Specify TC protection function
  tc-snooping              Specify TC snooping
  timer                    Specify timer configuration
  timer-factor             Specify aged out time factor
  vlan                     Virtual LAN

[Comware5]stp mode ?
  mstp  Multiple spanning tree protocol mode
  pvst  Per-VLAN spanning tree protocol mode
  rstp  Rapid spanning tree protocol mode
  stp   Spanning tree protocol mode
```

```
[Comware5]stp mode pvst


[Comware5]stp vlan ?
  INTEGER<1-4094>  Vlan ID

[Comware5]stp vlan 1 ?
  INTEGER<1-4094>  Vlan ID
  bridge-diameter  Specify bridge diameter
  enable           Enable spanning tree protocol
  priority         Specify bridge priority
  root             Specify root switch
  timer            Specify timer configuration
  to               Range of vlan

[Comware5]stp vlan 1 priority ?
  INTEGER<0-61440>  Bridge priority, in steps of 4096

[Comware5]stp vlan 1 priority 12288

[Comware5]stp vlan 220 priority 8192

[Comware5]stp vlan 100 priority 20480

[Comware5]stp vlan 240 priority 16384


[Comware5]stp enable


[Comware5]display stp ?
  abnormal-port         Display abnormal ports
  bpdu-statistics       STP BPDU statistics
  brief                 Brief information
  down-port             Port information of protocol down
  history               Root or alternate port history
  instance              Spanning tree instance
  interface             Specify interface
  region-configuration  Region configuration
  root                  Display status and configuration of the root bridge
  slot                  Slot Number
  tc                    Port TC count
  vlan                  Virtual LAN
  |                     Matching output
  <cr>

[Comware5]display stp root
VLAN  Root Bridge ID        ExtPathCost IntPathCost Root Port
    1  8192.009c-02d5-3980   0           20          GigabitEthernet1/0/6
  100  8192.cc3e-5f73-bacb   0           20020       GigabitEthernet1/0/6
  220  8192.0023-89d5-a059   0           0
  230  32768.0022-91ab-4380  0           20020       GigabitEthernet1/0/6
  240  8192.0022-91ab-4380   0           20020       GigabitEthernet1/0/6


[Comware5]display stp
-------[VLAN 1 Global Info]-------
Protocol Status     :enabled
Bridge ID           :12288.0023-89d5-a059
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s
Root ID / RPC       :8192.009c-02d5-3980 / 20
RootPortId          :128.6
BPDU-Protection     :disabled
```

```
TC or TCN received  :2
Time since last TC  :0 days 1h:7m:13s

 ----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=20
 Desg. Bridge/Port   :12288.0023-89d5-a059 / 128.1
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 Rapid transition    :true
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 1s

 ----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=20
 Desg. Bridge/Port   :8192.009c-02d5-3980 / 128.11
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 0s

-------[VLAN 100 Global Info]-------
Protocol Status     :enabled
Bridge ID           :20480.0023-89d5-a059
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s
Root ID / RPC       :8192.cc3e-5f73-bacb / 20020
RootPortId          :128.6
BPDU-Protection     :disabled
TC or TCN received  :6
Time since last TC  :0 days 1h:7m:33s

 ----[Port5(GigabitEthernet1/0/5)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=200
 Desg. Bridge/Port   :20480.0023-89d5-a059 / 128.5
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 Rapid transition    :false
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 2s

 ----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=20
 Desg. Bridge/Port   :16384.009c-02d5-3980 / 128.11
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 1s
```

```
 ----[Port9(GigabitEthernet1/0/9)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=200
 Desg. Bridge/Port   :20480.0023-89d5-a059 / 128.9
 Port Edged          :Config=enabled / Active=enabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 Rapid transition    :true
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 2s

-------[VLAN 220 Global Info]-------
Protocol Status     :enabled
Bridge ID           :8192.0023-89d5-a059
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s
Root ID / RPC       :8192.0023-89d5-a059 / 0
RootPortId          :0.0
BPDU-Protection     :disabled
TC or TCN received  :4
Time since last TC  :0 days 1h:7m:38s

 ----[Port5(GigabitEthernet1/0/5)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=200
 Desg. Bridge/Port   :8192.0023-89d5-a059 / 128.5
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 Rapid transition    :false
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 0s

 ----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=20
 Desg. Bridge/Port   :8192.0023-89d5-a059 / 128.6
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 Rapid transition    :true
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 0s

-------[VLAN 230 Global Info]-------
Protocol Status     :enabled
Bridge ID           :32768.0023-89d5-a059
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s
Root ID / RPC       :32768.0022-91ab-4380 / 20020
RootPortId          :128.6
BPDU-Protection     :disabled
TC or TCN received  :2
Time since last TC  :0 days 0h:40m:25s

 ----[Port5(GigabitEthernet1/0/5)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
```

```
 Port Cost(Legacy)    :Config=auto / Active=200
 Desg. Bridge/Port    :32768.0023-89d5-a059 / 128.5
 Port Edged           :Config=disabled / Active=disabled
 Point-to-point       :Config=auto / Active=true
 Transmit Limit       :10 packets/hello-time
 Protection Type      :None
 Rapid transition     :false
 PortTimes            :Hello 2s MaxAge 20s FwDly 15s MsgAge 2s

 ----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port Protocol        :enabled
 Port Role            :Root Port
 Port Priority        :128
 Port Cost(Legacy)    :Config=auto / Active=20
 Desg. Bridge/Port    :32768.009c-02d5-3980 / 128.11
 Port Edged           :Config=disabled / Active=disabled
 Point-to-point       :Config=auto / Active=true
 Transmit Limit       :10 packets/hello-time
 Protection Type      :None
 PortTimes            :Hello 2s MaxAge 20s FwDly 15s MsgAge 1s

-------[VLAN 240 Global Info]-------
Protocol Status      :enabled
Bridge ID            :16384.0023-89d5-a059
Bridge Times         :Hello 2s MaxAge 20s FwDly 15s
Root ID / RPC        :8192.0022-91ab-4380 / 20020
RootPortId           :128.6
BPDU-Protection      :disabled
TC or TCN received   :25
Time since last TC   :0 days 0h:53m:46s

 ----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port Protocol        :enabled
 Port Role            :Root Port
 Port Priority        :128
 Port Cost(Legacy)    :Config=auto / Active=20
 Desg. Bridge/Port    :20480.009c-02d5-3980 / 128.11
 Port Edged           :Config=disabled / Active=disabled
 Point-to-point       :Config=auto / Active=true
 Transmit Limit       :10 packets/hello-time
 Protection Type      :None
 PortTimes            :Hello 2s MaxAge 20s FwDly 15s MsgAge 1s
```

Comware7

```
[Comware7]stp ?
  bpdu-protection       Specify BPDU protection function
  bridge-diameter       Specify bridge diameter
  global                Specify global parameter
  instance              Specify the spanning tree instance list
  max-hops              Specify max hops
  mode                  Specify state machine mode
  pathcost-standard     Specify port path cost standard
  port-log              Specify port status logging
  priority              Specify bridge priority
  region-configuration  Enter MSTP region view
  root                  Specify root switch
  tc-protection         Specify TC protection function
  tc-snooping           Specify TC snooping
  timer                 Specify timer configuration
  timer-factor          Specify aged out time factor
  vlan                  Specify the VLAN list

[Comware7]stp mode ?
```

```
  mstp  Multiple spanning tree protocol mode
  pvst  Per-Vlan spanning tree mode
  rstp  Rapid spanning tree protocol mode
  stp   Spanning tree protocol mode

[Comware7]stp mode pvst


[Comware7]stp vlan ?
  INTEGER<1-4094>  Vlan ID

[Comware7]stp vlan 1 ?
  INTEGER<1-4094>  VLAN ID
  bridge-diameter  Specify bridge diameter
  enable           Enable STP in VLANs
  priority         Specify bridge priority
  root             Specify root switch
  timer            Specify timer configuration
  to               Range of VLAN

[Comware7]stp vlan 1 priority ?
  INTEGER<0-61440>  Bridge priority, in steps of 4096

[Comware7]stp vlan 1 priority 16384

[Comware7]stp vlan 220 priority 20480

[Comware7]stp vlan 100 priority 8192

[Comware7]stp vlan 240 priority 12288


[Comware7]stp global enable


[Comware7]display stp ?
  >                     Redirect it to a file
  >>                    Redirect it to a file in append mode
  abnormal-port         Display abnormal ports
  bpdu-statistics       BPDU statistics
  brief                 Brief information
  down-port             Port information of protocol down
  history               History of port roles
  instance              Specify the spanning tree instance list
  interface             Specify interface
  region-configuration  Region configuration
  root                  Display status and configuration of the root bridge
  slot                  Specify the slot number
  tc                    Port TC count
  vlan                  Specify the VLAN list
  |                     Matching output
  <cr>

[Comware7]display stp root
VLAN ID  Root Bridge ID        ExtPathCost IntPathCost Root Port
 1        8192.009c-02d5-3980   0           20          GE1/0/6
 100      8192.cc3e-5f73-bacb   0           0
 220      8192.0023-89d5-a059   0           20020       GE1/0/6
 230      32768.0022-91ab-4380  0           20020       GE1/0/6
 240      8192.0022-91ab-4380   0           20020       GE1/0/6


[Comware7]display stp
```

```
-------[VLAN 1 Global Info]-------
 Protocol status     : Enabled
 Bridge ID           : 16384.cc3e-5f73-bacb
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s
 VlanRoot ID/RPC     : 8192.009c-02d5-3980, 20
 RootPort ID         : 128.6
 BPDU-Protection     : Disabled
 TC or TCN received  : 0
 Time since last TC  : 0 days 2h:18m:16s

----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port
 Port ID             : 128.1
 Port cost(Legacy)   : Config=auto, Active=20
 Desg.bridge/port    : 16384.cc3e-5f73-bacb, 128.1
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 1s

----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Root Port
 Port ID             : 128.6
 Port cost(Legacy)   : Config=auto, Active=20
 Desg.bridge/port    : 8192.009c-02d5-3980, 128.13
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 0s

-------[VLAN 100 Global Info]-------
 Protocol status     : Enabled
 Bridge ID           : 8192.cc3e-5f73-bacb
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s
 VlanRoot ID/RPC     : 8192.cc3e-5f73-bacb, 0
 RootPort ID         : 0.0
 BPDU-Protection     : Disabled
 TC or TCN received  : 0
 Time since last TC  : 0 days 2h:19m:15s

----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port
 Port ID             : 128.6
 Port cost(Legacy)   : Config=auto, Active=20
 Desg.bridge/port    : 8192.cc3e-5f73-bacb, 128.6
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 0s

----[Port9(GigabitEthernet1/0/9)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port
 Port ID             : 128.9
```

```
 Port cost(Legacy)   : Config=auto, Active=200
 Desg.bridge/port    : 8192.cc3e-5f73-bacb, 128.9
 Port edged          : Config=enabled, Active=enabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 0s

-------[VLAN 220 Global Info]-------
 Protocol status     : Enabled
 Bridge ID           : 20480.cc3e-5f73-bacb
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s
 VlanRoot ID/RPC     : 8192.0023-89d5-a059, 20020
 RootPort ID         : 128.6
 BPDU-Protection     : Disabled
 TC or TCN received  : 0
 Time since last TC  : 0 days 2h:19m:15s

----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Root Port
 Port ID             : 128.6
 Port cost(Legacy)   : Config=auto, Active=20
 Desg.bridge/port    : 12288.009c-02d5-3980, 128.13
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 1s

-------[VLAN 230 Global Info]-------
 Protocol status     : Enabled
 Bridge ID           : 32768.cc3e-5f73-bacb
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s
 VlanRoot ID/RPC     : 32768.0022-91ab-4380, 20020
 RootPort ID         : 128.6
 BPDU-Protection     : Disabled
 TC or TCN received  : 0
 Time since last TC  : 0 days 2h:19m:15s

----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Root Port
 Port ID             : 128.6
 Port cost(Legacy)   : Config=auto, Active=20
 Desg.bridge/port    : 32768.009c-02d5-3980, 128.13
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 Protection type     : Config=none, Active=none
 Rapid transition    : False
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 1s

-------[VLAN 240 Global Info]-------
 Protocol status     : Enabled
 Bridge ID           : 12288.cc3e-5f73-bacb
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s
 VlanRoot ID/RPC     : 8192.0022-91ab-4380, 20020
 RootPort ID         : 128.6
 BPDU-Protection     : Disabled
 TC or TCN received  : 0
```

```
 Time since last TC  : 0 days 2h:19m:15s

----[Port6(GigabitEthernet1/0/6)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Root Port
 Port ID             : 128.6
 Port cost(Legacy)   : Config=auto, Active=20
 Desg.bridge/port    : 20480.009c-02d5-3980, 128.13
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 1s
```

Cisco

```
Cisco(config)#spanning-tree ?
  backbonefast  Enable BackboneFast Feature
  etherchannel  Spanning tree etherchannel specific configuration
  extend        Spanning Tree 802.1t extensions
  logging       Enable Spanning tree logging
  loopguard     Spanning tree loopguard options
  mode          Spanning tree operating mode
  mst           Multiple spanning tree configuration
  pathcost      Spanning tree pathcost options
  portfast      Spanning tree portfast options
  transmit      STP transmit parameters
  uplinkfast    Enable UplinkFast Feature
  vlan          VLAN Switch Spanning Tree

Cisco(config)#spanning-tree mode ?
  mst         Multiple spanning tree mode
  pvst        Per-Vlan spanning tree mode
  rapid-pvst  Per-Vlan rapid spanning tree mode

Cisco(config)#spanning-tree mode rapid-pvst
   (note - this is the default spanning-tree mode, command is shown for refernece)

Cisco(config)#spanning-tree vlan ?
  WORD  vlan range, example: 1,3-5,7,9-11

Cisco(config)#spanning-tree vlan 1 ?
  forward-time  Set the forward delay for the spanning tree
  hello-time    Set the hello interval for the spanning tree
  max-age       Set the max age interval for the spanning tree
  priority      Set the bridge priority for the spanning tree
  root          Configure switch as root
  <cr>

Cisco(config)#spanning-tree vlan 1 priority ?
  <0-61440>  bridge priority in increments of 4096

Cisco(config)#spanning-tree vlan 1 priority 20480

Cisco(config)#spanning-tree vlan 220 priority 16384

Cisco(config)#spanning-tree vlan 100 priority 12288

Cisco(config)#spanning-tree vlan 240 priority 8192


Cisco#show spanning-tree ?
  active             Report on active interfaces only
```

```
  backbonefast       Show spanning tree backbonefast status
  blockedports       Show blocked ports
  bridge             Status and configuration of this bridge
  detail             Detailed information
  inconsistentports  Show inconsistent ports
  interface          Spanning Tree interface status and configuration
  mst                Multiple spanning trees
  pathcost           Show Spanning pathcost options
  root               Status and configuration of the root bridge
  summary            Summary of port states
  uplinkfast         Show spanning tree uplinkfast status
  vlan               VLAN Switch Spanning Trees
  |                  Output modifiers
  <cr>

Cisco#show spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0230, VLAN0240
EtherChannel misconfig guard is enabled
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                      0         0        0          2          2
VLAN0100                      0         0        0          2          2
VLAN0220                      0         0        0          2          2
VLAN0230                      0         0        0          2          2
VLAN0240                      0         0        0          1          1
---------------------- -------- --------- -------- ---------- ----------
5 vlans                       0         0        0          9          9


Cisco#show spanning-tree root

                                          Root    Hello Max Fwd
Vlan                   Root ID            Cost    Time  Age Dly  Root Port
---------------- -------------------- --------- ----- --- ---  ------------
VLAN0001          8193 009c.02d5.3980         4    2   20  15  Gi1/0/6
VLAN0100          8292 cc3e.5f73.bacb     20004    2   20  15  Gi1/0/6
VLAN0220          8412 0023.89d5.a059     20004    2   20  15  Gi1/0/6
VLAN0230         32998 0022.91ab.4380         0    2   20  15
VLAN0240          8432 0022.91ab.4380         0    2   20  15
```

Chapter 24 RIP – v1 and v2

This chapter compares the commands you use to enable and configure Routing Information Protocol (RIP) v2.

RIP uses a distance vector (a number representing distance) to measure the cost of a given route. The cost is a distance vector because the cost often is equivalent to the number of router hops between the router and the destination network. A hop is another router through which packets must travel to reach the destination.

A RIP router can receive multiple paths to a destination. The software evaluates the paths, selects the best path, and saves the path in the IP route table as the route to the destination. Typically, the best path is the path with the fewest hops. If the router receives an RIP update from another router that contains a path with fewer hops than the path stored in the router's route table, the router replaces the older route with the newer one. The router then includes the new path in the updates it sends to other RIP routers.

RIP routers also can modify a route's cost, generally by adding to it, to bias the selection of a route for a given destination. In this case, the actual number of router hops may be the same, but the route has an administratively higher cost and is thus less likely to be used than other, lower-cost routes. A RIP route can have a maximum cost of 15. Any destination with a higher cost is considered unreachable. Although limiting to larger networks, the low maximum hop count prevents endless loops in the network.

RIP is a simple Interior Gateway Protocol (IGP), mainly used in small-sized networks, such as academic networks and simple LANs. It is not applicable to complex networks.

RIP has been widely used because it is easy to implement, configure, and maintain.

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# router rip ArubaOS-Switch(rip)# enable	[Comware]rip 1	Cisco(config)#router rip
ArubaOS-Switch(rip)# vlan 220 ip rip	[Comware-rip-1]network 10.1.220.0	Cisco(config-router)#network 10.1.220.0
	[Comware-rip-1]version 2	Cisco(config-router)#version 2
ArubaOS-Switch(rip)# redistribute connected	[Comware-rip-1]import-route direct	Cisco(config-router)#redistribute connected
ArubaOS-Switch# show ip rip	[Comware]display rip	Cisco#show ip rip database
ArubaOS-Switch# show ip rip interface vlan 220	[Comware]display rip 1 interface Vlan-interface 220 [Comware]display rip 1 database	Cisco#show ip rip database 10.1.220.0 255.255.255.0
ArubaOS-Switch# show ip rip redistribute		

ArubaOS-Switch

```
ArubaOS-Switch(config)# router rip

ArubaOS-Switch(rip)# enable

ArubaOS-Switch(rip)# vlan 220 ip rip


ArubaOS-Switch(rip)# redistribute connected


ArubaOS-Switch# show ip rip
 general                Show RIP basic configuration and operational information.
 interface              Show RIP interfaces' information.
 peer                   Show RIP peers.
 redistribute           List protocols which are being redistributed into RIP.
 restrict               List routes which will not be redistributed via RIP.
 <cr>

ArubaOS-Switch# show ip rip

 RIP global parameters

  RIP protocol   : enabled
  Auto-summary   : enabled
  Default Metric : 1
  Distance       : 120
  Route changes  : 0
  Queries        : 0

 RIP interface information

  IP Address      Status      Send mode        Recv mode  Metric      Auth
  --------------- ----------- ---------------- ---------- ----------- ----
  10.1.220.1      enabled     V2-only          V2-only    1           none

 RIP peer information

  IP Address      Bad routes  Last update timeticks
  --------------- ----------- ---------------------
  10.1.220.3      0           5


ArubaOS-Switch# show ip rip interface vlan 220

 RIP configuration and statistics for VLAN 220

 RIP interface information for 10.1.220.1

  IP Address : 10.1.220.1
  Status     : enabled

  Send mode  : V2-only
  Recv mode  : V2-only
  Metric : 1
  Auth : none

  Bad packets received : 0
  Bad routes received  : 0
  Sent updates : 0
```

```
ArubaOS-Switch# show ip rip redistribute

 RIP redistributing

 Route type RouteMap                        Options
 ---------- ------------------------------ ------------------
 connected
```

Comware

```
[Comware]rip 1

[Comware-rip-1]version 2

[Comware-rip-1]network 10.1.220.0

[Comware-rip-1]import-route direct


[Comware]display rip ?
  INTEGER<1-65535>  Process ID
  vpn-instance      VPN Instance
  |                 Matching output
  <cr>

[Comware]display rip
  Public VPN-instance name :

    RIP process : 1
       RIP version : 2
       Preference : 100
       Checkzero : Enabled
       Default-cost : 0
       Summary : Enabled
       Hostroutes : Enabled
       Maximum number of balanced paths : 8
       Update time   :   30 sec(s)  Timeout time         :  180 sec(s)
       Suppress time :  120 sec(s)  Garbage-collect time :  120 sec(s)
       update output delay :   20(ms)  output count :    3
       TRIP retransmit time :    5 sec(s)
       TRIP response packets retransmit count :   36
       Silent interfaces : None
       Default routes : Disabled
       Verify-source : Enabled
       Networks :
           10.0.0.0
       Configured peers : None
       Triggered updates sent : 20
       Number of routes changes : 25
       Number of replies to queries : 0


[Comware]display rip 1 ?
  database   Database
  interface  RIP interface information
  route      Route Information
  |          Matching output
  <cr>

[Comware]display rip 1 interface Vlan-interface 220


 Interface-name: Vlan-interface220
    Address/Mask:10.1.220.3/24       Version:RIPv2
```

```
    MetricIn:0                      MetricIn route policy:Not designated
    MetricOut:1                     MetricOut route policy:Not designated
    Split-horizon/Poison-reverse:on/off  Input/Output:on/on
    Default route:off
    Current packets number/Maximum packets number:0/2000


[Comware]display rip 1 database
   10.0.0.0/8, cost 0, ClassfulSumm
       10.0.111.0/24, cost 0, nexthop 10.0.111.31, Rip-interface
       10.1.100.0/24, cost 0, nexthop 10.1.100.3, Rip-interface
       10.1.220.0/24, cost 0, nexthop 10.1.220.3, Rip-interface
       10.1.230.0/24, cost 0, nexthop 10.1.230.3, Rip-interface
       10.1.240.0/24, cost 0, nexthop 10.1.240.3, Rip-interface
```

Cisco

```
Cisco(config)#router rip

Cisco(config-router)#network 10.1.220.0

Cisco(config-router)#version 2


Cisco(config-router)#redistribute connected


Cisco#show ip rip database
10.0.0.0/8    auto-summary
10.0.111.0/24    directly connected, Vlan1
10.1.100.0/24    directly connected, Vlan100
10.1.220.0/24    directly connected, Vlan220
10.1.230.0/24
    [1] via 10.1.240.3, 00:00:22, Vlan240
    [1] via 10.1.220.3, 00:00:22, Vlan220
    [1] via 10.1.100.3, 00:00:22, Vlan100
    [1] via 10.1.220.1, 00:00:05, Vlan220
10.1.240.0/24    directly connected, Vlan240


Cisco#show ip rip database 10.1.220.0 255.255.255.0
10.1.220.0/24    directly connected, Vlan220
```

Chapter 25 OSPFv2

This chapter compares the commands you use to enable and configure Open Shortest Path First (OSPF).

OSPF is a link-state routing protocol you can apply to routers grouped into OSPF areas identified by the routing configuration on each router. The protocol uses Link-State Advertisements (LSAs) transmitted by each router to update neighboring routers regarding that router's interfaces and the routes available through those interfaces.

Each router in an area also maintains a link-state database (LSDB) that describes the area topology. The routers used to connect areas to each other flood summary link LSAs and external link LSAs to neighboring OSPF areas to update them regarding available routes. In this way, each OSPF router determines the shortest path between itself and a desired destination router in the same OSPF domain (AS [Autonomous System]).

The OSPFv2 configurations in this chapter start with single area, then configuring multiple areas, afterwhich adding stub and totally stubby components, and then the show/display OSPF commands. Each section builds upon the next adding additional OSPF capabilities.

a) Single Area

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# ip router-id 10.0.0.21		
ArubaOS-Switch(config)# router ospf ArubaOS-Switch(ospf)# enable	[Comware]ospf 1 router-id 10.0.0.31	Cisco(config)#router ospf 1
		Cisco(config-router)#router-id 10.0.0.41
ArubaOS-Switch(ospf)# area 0	[Comware-ospf-1]area 0	
ArubaOS-Switch(ospf)# vlan 220 ArubaOS-Switch(vlan-220)# ip ospf area 0	[Comware-ospf-1-area-0.0.0.0]network 10.1.220.0 0.0.0.255	Cisco(config-router)#network 10.1.220.0 0.0.0.255 area 0
ArubaOS-Switch(vlan-220)# router ospf ArubaOS-Switch(ospf)# redistribute connected	[Comware-ospf-1]import-route direct	Cisco(config-router)#redistribute connected

ArubaOS-Switch
ArubaOS-Switch(config)# ip router-id 10.0.0.21   ArubaOS-Switch(config)# router ospf ArubaOS-Switch(ospf)# enable   ArubaOS-Switch(ospf)# area backbone

-or-

```
ArubaOS-Switch(ospf)# area 0.0.0.0
```

-or-

```
ArubaOS-Switch(ospf)# area 0


ArubaOS-Switch(ospf)# vlan 220

ArubaOS-Switch(vlan-220)# ip ospf area backbone
```

-or-

```
ArubaOS-Switch(vlan-220)# ip ospf area 0.0.0.0
```

-or-

```
ArubaOS-Switch(vlan-220)# ip ospf area 0

ArubaOS-Switch(vlan-220)# router ospf


(also as compound statements)

ArubaOS-Switch(config)# vlan 220 ip ospf area backbone
```

-or-

```
ArubaOS-Switch(config)# vlan 220 ip ospf area 0
```

-or-

```
ArubaOS-Switch(config)# vlan 220 ip ospf area 0.0.0.0


ArubaOS-Switch(ospf)# redistribute ?
 connected
 static
 rip
 bgp

ArubaOS-Switch(ospf)# redistribute connected
```

Comware

```
[Comware]ospf 1 router-id 10.0.0.31


[Comware-ospf-1]area 0
```

-or-

```
[Comware-ospf-1]area 0.0.0.0


[Comware-ospf-1-area-0.0.0.0]network 10.1.220.0 0.0.0.255


[Comware-ospf-1]import-route ?
  bgp     Border Gateway Protocol (BGP) routes
  direct  Direct routes
  isis    Intermediate System to Intermediate System (IS-IS) routes
  ospf    Open Shortest Path First (OSPF) routes
  rip     Routing Information Protocol (RIP) routes
  static  Static routes

[Comware-ospf-1]import-route direct
```

Cisco

```
Cisco(config)#router ospf 1


Cisco(config-router)#router-id 10.0.0.41
```

```
Cisco(config-router)#network 10.1.220.0 0.0.0.255 area 0
-or-
Cisco(config-router)#network 10.1.220.0 0.0.0.255 area 0.0.0.0


Cisco(config-router)#redistribute ?
  bgp             Border Gateway Protocol (BGP)
  connected       Connected
  eigrp           Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis            ISO IS-IS
  iso-igrp        IGRP for OSI networks
  maximum-prefix  Maximum number of prefixes redistributed to protocol
  metric          Metric for redistributed routes
  metric-type     OSPF/IS-IS exterior metric type for redistributed routes
  mobile          Mobile routes
  nssa-only       Limit redistributed routes to NSSA areas
  odr             On Demand stub Routes
  ospf            Open Shortest Path First (OSPF)
  rip             Routing Information Protocol (RIP)
  route-map       Route map reference
  static          Static routes
  subnets         Consider subnets for redistribution into OSPF
  tag             Set tag for routes redistributed into OSPF
  <cr>

Cisco(config-router)#redistribute connected
```

b) Multiple Areas

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# router ospf	[Comware]ospf 1	Cisco(config)#router ospf 1
ArubaOS-Switch(ospf)# area 1	[Comware-ospf-1]area 1	
ArubaOS-Switch(ospf)# area 2		
ArubaOS-Switch(ospf)# vlan 100 ArubaOS-Switch(vlan-100)# ip ospf area 1	[Comware-ospf-1-area-0.0.0.1]network 10.1.100.0 0.0.0.255	Cisco(config-router)#network 10.1.100.0 0.0.0.255 area 1
	[Comware-ospf-1-area-0.0.0.1]area 2	
ArubaOS-Switch(vlan-100)# vlan 230 ArubaOS-Switch(vlan-230)# ip ospf area 2	[Comware-ospf-1-area-0.0.0.2]network 10.1.230.0 0.0.0.255	Cisco(config-router)#network 10.1.230.0 0.0.0.255 area 2

ArubaOS-Switch

```
ArubaOS-Switch(config)# router ospf


ArubaOS-Switch(ospf)# area 1
  -or-
ArubaOS-Switch(ospf)# area 0.0.0.1


ArubaOS-Switch(ospf)# area 2
  -or-
ArubaOS-Switch(ospf)# area 0.0.0.2


ArubaOS-Switch(ospf)# vlan 100

ArubaOS-Switch(vlan-100)# ip ospf area 1
  -or-
ArubaOS-Switch(vlan-100)# ip ospf area 0.0.0.1


ArubaOS-Switch(vlan-100)# vlan 230

ArubaOS-Switch(vlan-230)# ip ospf area 2
  -or-
ArubaOS-Switch(vlan-230)# ip ospf area 0.0.0.2


(also as compound statements)

ArubaOS-Switch(config)# vlan 100 ip ospf area 1
  -or-
ArubaOS-Switch(config)# vlan 100 ip ospf area 0.0.0.1


ArubaOS-Switch(config)# vlan 230 ip ospf area 2
  -or-
ArubaOS-Switch(config)# vlan 230 ip ospf area 0.0.0.2
```

Comware
[Comware]ospf 1 [Comware-ospf-1]area 1 -or- [Comware-ospf-1]area 0.0.0.1 [Comware-ospf-1-area-0.0.0.1]network 10.1.100.0 0.0.0.255 [Comware-ospf-1-area-0.0.0.1]area 2 -or- [Comware-ospf-1-area-0.0.0.1]area 0.0.0.2 [Comware-ospf-1-area-0.0.0.2]network 10.1.230.0 0.0.0.255
Cisco
Cisco(config)#router ospf 1 Cisco(config-router)#network 10.1.100.0 0.0.0.255 area 1 -or- Cisco(config-router)#network 10.1.100.0 0.0.0.255 area 0.0.0.1 Cisco(config-router)#network 10.1.230.0 0.0.0.255 area 2 -or- Cisco(config-router)#network 10.1.230.0 0.0.0.255 area 0.0.0.2

c) Stub

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(ospf)# area 1 stub 11	[Comware-ospf-1]area 1 [Comware-ospf-1-area-0.0.0.1]stub	Cisco(config-router)#area 1 stub

ArubaOS-Switch
ArubaOS-Switch(ospf)# area 1 stub 11
Comware
[Comware-ospf-1]area 1 [Comware-ospf-1-area-0.0.0.1]stub
Cisco
Cisco(config-router)#area 1 stub

d) Totally Stubby

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(ospf)# area 2 stub no-summary 11	[Comware-ospf-1]area 2 [Comware-ospf-1-area-0.0.0.2]stub no-summary	Cisco(config-router)#area 2 stub no-summary
ArubaOS-Switch(config)# vlan 230	[Comware]interface Vlan-interface 230	Cisco(config-if)#interface vlan 230
ArubaOS-Switch(vlan-230)# ip ospf cost 10	[Comware-Vlan-interface230]ospf cost 10	Cisco(config-if)#ip ospf cost 10

ArubaOS-Switch

```
ArubaOS-Switch(ospf)# area 2 stub no-summary 11


ArubaOS-Switch(config)# vlan 230

ArubaOS-Switch(vlan-230)# ip ospf cost 10
```

Comware

```
[Comware-ospf-1]area 2

[Comware-ospf-1-area-0.0.0.2]stub no-summary



[Comware]interface Vlan-interface 230

[Comware-Vlan-interface230]ospf cost 10
```

Cisco

```
Cisco(config-router)#area 2 stub no-summary


Cisco(config-if)#interface vlan 230

Cisco(config-if)#ip ospf cost 10
```

e) Show or Display OSPF Commands

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch# show ip ospf interface	[Comware]display ospf interface	Cisco#show ip ospf interface brief
ArubaOS-Switch# show ip ospf neighbor	[Comware]display ospf peer	Cisco#show ip ospf neighbor
ArubaOS-Switch# show ip ospf link-state	[Comware]display ospf lsdb	Cisco#show ip ospf database

ArubaOS-Switch

```
ArubaOS-Switch# show ip ospf ?
 area                   Show OSPF areas configured on the device.
 external-link-state    Show the Link State Advertisements from throughout the areas to
                        which the device is attached.
 general                Show OSPF basic configuration and operational information.
 interface              Show OSPF interfaces' information.
 link-state             Show all Link State Advertisements from throughout the areas to
                        which the device is attached.
 neighbor               Show all OSPF neighbors in the locality of of the device.
 redistribute           List protocols which are being redistributed into OSPF.
 restrict               List routes which will not be redistributed via OSPF.
 spf-log                List the OSPF SPF(Shortes Path First Algorithm) run count for all
                        OSPF areas and last ten Reasons for running SPF.
 statistics             List OSPF packet statistics( OSPF sent,recieved and error packet
                        count) of all OSPF enabled interfaces.
 traps                  Show OSPF traps enabled on the device.
 virtual-link           Show status of all OSPF virtual links configured.
 virtual-neighbor       Show all virtual neighbors of the device.
 <cr>


ArubaOS-Switch# show ip ospf interface

 OSPF Interface Status

  IP Address      Status   Area ID         State    Auth-type Cost  Pri Passive
  --------------- -------- --------------- -------- --------- ----- --- -------
  10.1.100.1      enabled  0.0.0.1         DR       none      1     1   no
  10.1.220.1      enabled  backbone        DR       none      1     1   no
  10.1.230.1      enabled  0.0.0.2         DROTHER  none      1     1   no


ArubaOS-Switch# show ip ospf neighbor

 OSPF Neighbor Information

                                                        Rxmt         Helper
  Router ID       Pri IP Address      NbIfState State    QLen  Events Status
  --------------- --- --------------- --------- -------- ----- ------ ------
  10.0.0.31       1   10.1.100.3      BDR       FULL     0     7      None
  10.0.0.41       1   10.1.100.4                FULL     0     13     None
  10.0.0.51       1   10.1.100.5                FULL     0     7      None
  10.0.0.31       1   10.1.220.3      BDR       FULL     0     7      None
  10.0.0.41       1   10.1.220.4                FULL     0     7      None
  10.0.0.51       1   10.1.220.5                FULL     0     7      None
  10.0.0.31       1   10.1.230.3      BDR       FULL     0     11     None
  10.0.0.41       1   10.1.230.4      DR        FULL     0     7      None
  10.0.0.51       1   10.1.230.5                2WAY     0     3      None
```

```
ArubaOS-Switch# show ip ospf link-state

 OSPF Link State Database for Area 0.0.0.0

                              Advertising
  LSA Type    Link State ID   Router ID       Age  Sequence #  Checksum
  ----------- --------------- --------------- ---- ----------- ----------
  Router      10.0.0.21       10.0.0.21       313  0x8000000e  0x0000b05e
  Router      10.0.0.31       10.0.0.31       468  0x80000012  0x0000060f
  Router      10.0.0.41       10.0.0.41       474  0x80000004  0x0000ad40
  Router      10.0.0.51       10.0.0.51       315  0x80000015  0x00001790
  Network     10.1.220.5      10.0.0.51       315  0x80000004  0x0000d754
  Summary     10.1.100.0      10.0.0.21       322  0x80000001  0x0000dbd1
  Summary     10.1.100.0      10.0.0.31       91   0x80000004  0x00007b45
  Summary     10.1.100.0      10.0.0.41       1439 0x80000009  0x0000533e
  Summary     10.1.100.0      10.0.0.51       662  0x80000009  0x00003532
  Summary     10.1.230.0      10.0.0.21       323  0x80000001  0x00009a87
  Summary     10.1.230.0      10.0.0.31       821  0x80000003  0x00003cf9
  Summary     10.1.230.0      10.0.0.41       853  0x80000008  0x000014f2
  Summary     10.1.230.0      10.0.0.51       840  0x80000003  0x0000ffe1

 OSPF Link State Database for Area 0.0.0.1

                              Advertising
  LSA Type    Link State ID   Router ID       Age  Sequence #  Checksum
  ----------- --------------- --------------- ---- ----------- ----------
  Router      10.0.0.21       10.0.0.21       312  0x80000011  0x00006898
  Router      10.0.0.31       10.0.0.31       471  0x80000015  0x0000bd49
  Router      10.0.0.41       10.0.0.41       1451 0x80000002  0x00006f75
  Router      10.0.0.51       10.0.0.51       314  0x8000001b  0x0000c8cd
  Network     10.1.100.5      10.0.0.51       314  0x80000007  0x00001d86
  Summary     0.0.0.0         10.0.0.21       325  0x80000001  0x00003dd7
  Summary     0.0.0.0         10.0.0.31       90   0x80000003  0x00007ab8
  Summary     0.0.0.0         10.0.0.41       1454 0x80000001  0x000060aa
  Summary     0.0.0.0         10.0.0.51       765  0x80000002  0x0000409f
  Summary     10.1.220.0      10.0.0.21       315  0x80000009  0x0000bc72
  Summary     10.1.220.0      10.0.0.31       94   0x80000009  0x000062e2
  Summary     10.1.220.0      10.0.0.41       1447 0x80000009  0x000044d6
  Summary     10.1.220.0      10.0.0.51       760  0x80000008  0x000028c9
  Summary     10.1.230.0      10.0.0.21       316  0x8000000d  0x0000a077
  Summary     10.1.230.0      10.0.0.31       826  0x80000002  0x00005cdc
  Summary     10.1.230.0      10.0.0.41       858  0x80000009  0x000030d7
  Summary     10.1.230.0      10.0.0.51       844  0x8000000c  0x00000cce

 OSPF Link State Database for Area 0.0.0.2

                              Advertising
  LSA Type    Link State ID   Router ID       Age  Sequence #  Checksum
  ----------- --------------- --------------- ---- ----------- ----------
  Router      10.0.0.21       10.0.0.21       324  0x80000013  0x000034bd
  Router      10.0.0.31       10.0.0.31       328  0x80000019  0x00008570
  Router      10.0.0.41       10.0.0.41       865  0x80000006  0x0000379c
  Router      10.0.0.51       10.0.0.51       844  0x8000001b  0x000098f0
  Network     10.1.230.4      10.0.0.41       323  0x80000003  0x00003917
  Summary     0.0.0.0         10.0.0.21       330  0x80000001  0x00003dd7
  Summary     0.0.0.0         10.0.0.31       959  0x80000001  0x00007eb6
  Summary     0.0.0.0         10.0.0.41       883  0x80000001  0x000060aa
  Summary     0.0.0.0         10.0.0.51       910  0x80000001  0x0000429e
```

Comware

```
[Comware]display ospf ?
  INTEGER<1-65535>  Process ID
```

```
  abr-asbr          Information of the OSPF ABR and ASBR
  asbr-summary      Information of aggregate addresses for OSPF(only for ASBR)
  brief             brief information of OSPF processes
  cumulative        Statistics information
  error             Error information
  interface         Interface information
  lsdb              Link state database
  nexthop           Nexthop information
  peer              Specify a neighbor router
  request-queue     Link state request list
  retrans-queue     Link state retransmission list
  routing           OSPF route table
  sham-link         Sham Link
  vlink             Virtual link information


[Comware]display ospf interface

         OSPF Process 1 with Router ID 10.0.0.31
                 Interfaces

 Area: 0.0.0.0
 IP Address      Type      State    Cost  Pri   DR              BDR
 10.1.220.3      Broadcast BDR      1     1     10.1.220.1      10.1.220.3

 Area: 0.0.0.1
 IP Address      Type      State    Cost  Pri   DR              BDR
 10.1.100.3      Broadcast BDR      1     1     10.1.100.1      10.1.100.3

 Area: 0.0.0.2
 IP Address      Type      State    Cost  Pri   DR              BDR
 10.1.230.3      Broadcast BDR      1     1     10.1.230.4      10.1.230.3


[Comware]display ospf peer

                  OSPF Process 1 with Router ID 10.0.0.31
                        Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri  Dead-Time  Interface       State
 10.0.0.21       10.1.220.1      1    36         Vlan220         Full/DR
 10.0.0.41       10.1.220.4      1    34         Vlan220         Full/DROther
 10.0.0.51       10.1.220.5      1    32         Vlan220         Full/DROther

 Area: 0.0.0.1
 Router ID       Address         Pri  Dead-Time  Interface       State
 10.0.0.21       10.1.100.1      1    35         Vlan100         Full/DR
 10.0.0.41       10.1.100.4      1    40         Vlan100         Full/DROther
 10.0.0.51       10.1.100.5      1    36         Vlan100         Full/DROther

 Area: 0.0.0.2
 Router ID       Address         Pri  Dead-Time  Interface       State
 10.0.0.21       10.1.230.1      1    30         Vlan230         Full/DROther
 10.0.0.41       10.1.230.4      1    40         Vlan230         Full/DR
 10.0.0.51       10.1.230.5      1    39         Vlan230         Full/DROther


[Comware]display ospf lsdb

         OSPF Process 1 with Router ID 10.0.0.31
                 Link State Database
```

```
                        Area: 0.0.0.0
Type       LinkState ID    AdvRouter          Age  Len   Sequence   Metric
Router     10.0.0.41       10.0.0.41          540  36    80000004       0
Router     10.0.0.51       10.0.0.51          383  36    80000015       0
Router     10.0.0.31       10.0.0.31          536  36    80000012       0
Router     10.0.0.21       10.0.0.21          385  36    8000000E       0
Network    10.1.220.5      10.0.0.51          384  40    80000004       0
Sum-Net    10.1.230.0      10.0.0.31          887  28    80000003      10
Sum-Net    10.1.230.0      10.0.0.51          906  28    80000003      10
Sum-Net    10.1.230.0      10.0.0.41          920  28    80000008      10
Sum-Net    10.1.230.0      10.0.0.21          393  28    80000001      10
Sum-Net    10.1.100.0      10.0.0.31          159  28    80000004       1
Sum-Net    10.1.100.0      10.0.0.51          730  28    80000009       1
Sum-Net    10.1.100.0      10.0.0.41         1507  28    80000009       1
Sum-Net    10.1.100.0      10.0.0.21          393  28    80000001       1
                        Area: 0.0.0.1
Type       LinkState ID    AdvRouter          Age  Len   Sequence   Metric
Router     10.0.0.41       10.0.0.41         1518  36    80000002       0
Router     10.0.0.51       10.0.0.51          381  36    8000001B       0
Router     10.0.0.31       10.0.0.31          537  36    80000015       0
Router     10.0.0.21       10.0.0.21          382  36    80000011       0
Network    10.1.100.5      10.0.0.51          382  40    80000007       0
Sum-Net    0.0.0.0         10.0.0.51          832  28    80000002       1
Sum-Net    0.0.0.0         10.0.0.41         1522  28    80000001       1
Sum-Net    0.0.0.0         10.0.0.31          157  28    80000003       1
Sum-Net    0.0.0.0         10.0.0.21          395  28    80000001      11
Sum-Net    10.1.230.0      10.0.0.51          908  28    8000000C      10
Sum-Net    10.1.230.0      10.0.0.21          383  28    8000000D      10
Sum-Net    10.1.230.0      10.0.0.41          922  28    80000009      10
Sum-Net    10.1.230.0      10.0.0.31          889  28    80000002      10
Sum-Net    10.1.220.0      10.0.0.31          159  28    80000009       1
Sum-Net    10.1.220.0      10.0.0.51          827  28    80000008       1
Sum-Net    10.1.220.0      10.0.0.21          384  28    80000009       1
Sum-Net    10.1.220.0      10.0.0.41         1513  28    80000009       1
                        Area: 0.0.0.2
Type       LinkState ID    AdvRouter          Age  Len   Sequence   Metric
Router     10.0.0.41       10.0.0.41          930  36    80000006       0
Router     10.0.0.51       10.0.0.51          909  36    8000001B       0
Router     10.0.0.31       10.0.0.31          393  36    80000019       0
Router     10.0.0.21       10.0.0.21          390  36    80000013       0
Network    10.1.230.4      10.0.0.41          388  40    80000003       0
Sum-Net    0.0.0.0         10.0.0.31         1023  28    80000001       1
Sum-Net    0.0.0.0         10.0.0.51          974  28    80000001       1
Sum-Net    0.0.0.0         10.0.0.41          948  28    80000001       1
Sum-Net    0.0.0.0         10.0.0.21          398  28    80000001      11

                AS External Database
Type       LinkState ID    AdvRouter          Age  Len   Sequence   Metric
External   10.0.111.0      10.0.0.31          160  36    80000009       1
External   10.1.220.0      10.0.0.31          180  36    80000002       1
External   10.1.240.0      10.0.0.31          180  36    80000002       1
External   10.1.100.0      10.0.0.31          178  36    80000002       1
External   10.1.230.0      10.0.0.31          176  36    80000002       1
External   10.0.111.0      10.0.0.51          933  36    80000008       1
External   10.0.111.0      10.0.0.21          390  36    80000008      10
External   10.1.220.0      10.0.0.51          933  36    80000008       1
External   10.1.240.0      10.0.0.51          934  36    80000008       1
External   10.1.240.0      10.0.0.21          391  36    80000008      10
External   10.1.100.0      10.0.0.51          934  36    80000008       1
External   10.1.230.0      10.0.0.51          394  36    80000008       1
```

Cisco

```
Cisco#show ip ospf ?
  <1-65535>            Process ID number
  border-routers       Border and Boundary Router Information
  database             Database summary
  events               OSPF event information
  flood-list           Link state flood list
  interface            Interface information
  max-metric           Max-metric origination information
  mpls                 MPLS related information
  neighbor             Neighbor list
  nsf                  NSF state information
  request-list         Link state request list
  retransmission-list  Link state retransmission list
  rib                  Routing Information Base (RIB)
  sham-links           Sham link information
  statistics           Various OSPF Statistics
  summary-address      Summary-address redistribution Information
  timers               OSPF timers information
  topology-info        Topology Info
  traffic              Traffic related statistics
  virtual-links        Virtual link information
  |                    Output modifiers
  <cr>


Cisco#show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Vl220        1     0               10.1.220.4/24      1     DROTH 2/3
Vl100        1     1               10.1.100.4/24      1     DROTH 2/3
Vl230        1     0.0.0.2         10.1.230.4/24      1     DR    3/3


Cisco#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.0.0.21         1   FULL/DR         00:00:36    10.1.220.1      Vlan220
10.0.0.31         1   FULL/BDR        00:00:38    10.1.220.3      Vlan220
10.0.0.51         1   2WAY/DROTHER    00:00:34    10.1.220.5      Vlan220
10.0.0.21         1   FULL/DR         00:00:36    10.1.100.1      Vlan100
10.0.0.31         1   FULL/BDR        00:00:34    10.1.100.3      Vlan100
10.0.0.51         1   2WAY/DROTHER    00:00:38    10.1.100.5      Vlan100
10.0.0.21         1   FULL/DROTHER    00:00:32    10.1.230.1      Vlan230
10.0.0.31         1   FULL/BDR        00:00:38    10.1.230.3      Vlan230
10.0.0.51         1   FULL/DROTHER    00:00:31    10.1.230.5      Vlan230


Cisco#show ip ospf database

            OSPF Router with ID (10.0.0.41) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.0.0.21       10.0.0.21       474         0x8000000E 0x00B05E 1
10.0.0.31       10.0.0.31       626         0x80000012 0x00060F 1
10.0.0.41       10.0.0.41       630         0x80000004 0x00AD40 1
10.0.0.51       10.0.0.51       473         0x80000015 0x001790 1

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.220.5      10.0.0.51       473         0x80000004 0x00D754
```

```
                Summary Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.100.0      10.0.0.21       482         0x80000001 0x00DBD1
10.1.100.0      10.0.0.31       249         0x80000004 0x007B45
10.1.100.0      10.0.0.41       1594        0x80000009 0x00533E
10.1.100.0      10.0.0.51       819         0x80000009 0x003532
10.1.230.0      10.0.0.21       482         0x80000001 0x009A87
10.1.230.0      10.0.0.31       978         0x80000003 0x003CF9
10.1.230.0      10.0.0.41       1007        0x80000008 0x0014F2
10.1.230.0      10.0.0.51       995         0x80000003 0x00FFE1

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.0.0.21       10.0.0.21       470         0x80000011 0x006898 1
10.0.0.31       10.0.0.31       626         0x80000015 0x00BD49 1
10.0.0.41       10.0.0.41       1604        0x80000002 0x006F75 1
10.0.0.51       10.0.0.51       469         0x8000001B 0x00C8CD 1

                Net Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.100.5      10.0.0.51       469         0x80000007 0x001D86

                Summary Net Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
0.0.0.0         10.0.0.21       482         0x80000001 0x003DD7
0.0.0.0         10.0.0.31       245         0x80000003 0x007AB8
0.0.0.0         10.0.0.41       1608        0x80000001 0x0060AA
0.0.0.0         10.0.0.51       919         0x80000002 0x00409F
10.1.220.0      10.0.0.21       470         0x80000009 0x00BC72
10.1.220.0      10.0.0.31       247         0x80000009 0x0062E2
10.1.220.0      10.0.0.41       1598        0x80000009 0x0044D6
10.1.220.0      10.0.0.51       913         0x80000008 0x0028C9
10.1.230.0      10.0.0.21       470         0x8000000D 0x00A077
10.1.230.0      10.0.0.31       978         0x80000002 0x005CDC
10.1.230.0      10.0.0.41       1007        0x80000009 0x0030D7
10.1.230.0      10.0.0.51       995         0x8000000C 0x000CCE

                Router Link States (Area 0.0.0.2)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.0.0.21       10.0.0.21       477         0x80000013 0x0034BD 1
10.0.0.31       10.0.0.31       480         0x80000019 0x008570 1
10.0.0.41       10.0.0.41       1015        0x80000006 0x00379C 1
10.0.0.51       10.0.0.51       996         0x8000001B 0x0098F0 1

                Net Link States (Area 0.0.0.2)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.230.4      10.0.0.41       473         0x80000003 0x003917

                Summary Net Link States (Area 0.0.0.2)

Link ID         ADV Router      Age         Seq#       Checksum
0.0.0.0         10.0.0.21       482         0x80000001 0x003DD7
0.0.0.0         10.0.0.31       1110        0x80000001 0x007EB6
0.0.0.0         10.0.0.41       1032        0x80000001 0x0060AA
0.0.0.0         10.0.0.51       1061        0x80000001 0x00429E
```

```
                 Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
10.0.111.0      10.0.0.21       474         0x80000008 0x0032D6 0
10.0.111.0      10.0.0.31       245         0x80000009 0x008D98 1
10.0.111.0      10.0.0.51       1017        0x80000008 0x00537F 1
10.1.100.0      10.0.0.31       263         0x80000002 0x00092E 1
10.1.100.0      10.0.0.51       1017        0x80000008 0x00C01C 1
10.1.220.0      10.0.0.31       265         0x80000002 0x00DBE2 1
10.1.220.0      10.0.0.51       1017        0x80000008 0x0093D0 1
10.1.230.0      10.0.0.31       261         0x80000002 0x006D47 1
10.1.230.0      10.0.0.51       477         0x80000008 0x002535 1
10.1.240.0      10.0.0.21       474         0x80000008 0x0095F0 0
10.1.240.0      10.0.0.31       265         0x80000002 0x00FEAB 1
10.1.240.0      10.0.0.51       1017        0x80000008 0x00B699 1
```

Chapter 26 BGP version 4

This chapter compares the commands used to enable and configure Border Gateway Protocol version 4 (also referenced as: BGP-4, BGP4, BGPv4).

BGP, based on RFC 4271, is a routing protocol that enables BGP-speaking devices to exchange reachability information about independent networks called Autonomous Systems (ASs). These networks present themselves to other ASs as independent entities that have a single, coherent routing plan. BGP is the most commonly used protocol between Internet service providers (ISPs).

The characteristics of BGP are as follows:

- BGP focuses on the control of route propagation and the selection of optimal routes, rather than on route discovery and calculation, which makes BGP an exterior gateway protocol, different from interior gateway protocols such as Open Shortest Path First (OSPF) and Routing Information Protocol (RIP).
- BGP uses TCP to enhance reliability.
- BGP supports Classless Inter-Domain Routing (CIDR).
- BGP reduces bandwidth consumption by advertising only incremental updates, and is therefore used to advertise a large amount of routing information on the Internet.
- BGP eliminates routing loops completely by adding AS path information to BGP routes.
- BGP provides abundant policies to implement flexible route filtering and selection.
- BGP is scalable.

A router advertising BGP messages is called a BGP speaker. It establishes peer relationships with other BGP speakers to exchange routing information. When a BGP speaker receives a new route or a route better than the current one from another AS, it will advertise the route to all the other BGP peers in the local AS.

BGP can be configured to run on a router in the following two modes:

- iBGP (internal BGP)
- eBGP (external BGP)

When a BGP speaker peers with another BGP speaker that resides in the same AS, the session is referred to as an iBGP session; and, when a BGP speaker peers with a BGP speaker that resides in another AS, the session is referred to as an eBGP session.

a) eBGP

ArubaOS-Switch	Comware5	Cisco
ArubaOS-Switch(config)# router bgp 64502	[Comware5]bgp 64503	Cisco(config)#router bgp 64504
ArubaOS-Switch(bgp)# bgp router-id 10.0.0.2	[Comware5-bgp]router-id 10.0.0.3	Cisco(config-router)#bgp router-id 10.0.0.4
ArubaOS-Switch(bgp)# neighbor 10.0.101.31 remote-as 64503	[Comware5-bgp]peer 10.0.101.21 as-number 64502	Cisco(config-router)#neighbor 10.0.101.21 remote-as 64502
ArubaOS-Switch(bgp)# neighbor 10.0.101.41 remote-as 64504		
ArubaOS-Switch(bgp)# neighbor 10.0.101.51 remote-as 64505		
ArubaOS-Switch(bgp)# redistribute connected	[Comware5-bgp]import-route direct	Cisco(config-router)#redistribute connected
ArubaOS-Switch(bgp)# redistribute static		
ArubaOS-Switch(bgp)# enable		
ArubaOS-Switch(bgp)# network 10.0.221.0/24	[Comware5-bgp]network 10.0.231.0 24	Cisco(config-router)#network 10.0.241.0 mask 255.255.255.0
ArubaOS-Switch# show ip bgp summary	[Comware5]display bgp peer	Cisco#show ip bgp summary
	Comware7	
	[Comware7]bgp 64505	
	[Comware7-bgp]router-id 10.0.0.5	
	[Comware7-bgp]peer 10.0.101.21 as-number 64502	
	[Comware7-bgp]address-family ipv4 unicast	
	[Comware7-bgp-ipv4]peer 10.0.101.21 enable	
	[Comware7-bgp-ipv4]import-route direct	
	[Comware7-bgp-ipv4]network 10.0.251.0 24	
	[Comware7]display bgp peer ipv4	

ArubaOS-Switch

```
ArubaOS-Switch(config)# router bgp ?
 <1-65535>              The autonomous system number for the BGP routing process on this
                        router

ArubaOS-Switch(config)# router bgp 64502 ?
 bgp                    Configure various BGP parameters.
 disable                Disable BGP on the router.
 distance               Configure the administrative distances for BGP routes.
 enable                 Enable BGP on the router.
 neighbor               Add/Modify/delete entries of the BGP peer table.
 network                Advertise a network to the BGP neighbors if the network exists in
                        the routing table.
 redistribute           Advertises routes from the specified protocol to the BGP
                        neighbors.
 timers                 Configure global keepalive and hold-time values for BGP.
```

```
 <cr>

ArubaOS-Switch(config)# router bgp 64502


ArubaOS-Switch(bgp)# bgp
 allowas-in            Specify the number of times the local AS may appear in an AS-path.
 always-compare-med    Compare MEDs for routes from neighbors in different ASs.
 bestpath              Configure various BGP best-path options.
 client-to-client-r... Enable or Disable client-to-client route reflection.
 cluster-id            Specify the cluster ID to be used when the BGP router is used as a
                       route-reflector.
 default-metric        Specify a BGP MED to be set on routes when they are advertised to
                       peers.
 graceful-restart      Configure BGP graceful restart timers.
 log-neighbor-changes  Enable or disable BGP event logging.
 maximum-prefix        Specify the maximum number of routes that BGP will add to its
                       routing table.
 open-on-accept        Configure BGP to send an Open message immediately when the TCP
                       connection has been established for configured peers.
 router-id             Configure a BGP router-id to be used during neighbor session
                       establishment and in BGP best-path selection.

ArubaOS-Switch(bgp)# bgp router-id ?
 IP-ADDR               A 32-bit integer in ipv4-address format to be used as the BGP
                       router-id

ArubaOS-Switch(bgp)# bgp router-id 10.0.0.2


ArubaOS-Switch(bgp)# ?
 bgp                   Configure various BGP parameters.
 disable               Disable BGP on the router.
 distance              Configure the administrative distances for BGP routes.
 enable                Enable BGP on the router.
 neighbor              Add/Modify/delete entries of the BGP peer table.
 network               Advertise a network to the BGP neighbors if the network exists in
                       the routing table.
 redistribute          Advertises routes from the specified protocol to the BGP
                       neighbors.
 timers                Configure global keepalive and hold-time values for BGP.

ArubaOS-Switch(bgp)# neighbor 10.0.101.31 ?
 allowas-in            Specify the number of times the local AS # may appear in an
                       AS-path.
 as-override           Replace all occurrences of the peer AS number with the router's
                       own AS number before advertising the route.
 description           Configure description for this BGP peer or peer-group.
 dynamic               Enable or disable advertisement of dynamic capability to the peer.
 ebgp-multihop         Enable or disable multi-hop peering with the specified EBGP peer,
                       and optionally indicate the maximum number of hops (TTL).
 graceful-restart      Enable or Disable the advertisement of graceful-restart
                       capability.
 ignore-leading-as     Allow any received routes that do not have their own AS appended
                       to the as-path.
 local-as              Configure the local AS # used for peering with this peer .
 maximum-prefix        Specify the maximum number of routes BGP will accept from the
                       specified peer.
 next-hop-self         Force BGP to use the router's outbound interface address as the
                       next hop for the route updates to the peer.
 out-delay             Specify the delay-time before advertising the route updates to the
                       peer.
 passive               If enabled, do not initiate a peering connection to the peer.
```

```
 password               Use MD5 authentication for the peer and set the password to be
                        used. If in enhanced secure-mode, you will be prompted for the
                        password.
 remote-as              Add an entry to the neighbor table, specifying the AS # of the BGP
                        peer.
 remove-private-as      Specify whether the private AS # should be removed from the
                        as-path attribute of updates to the EBGP peer.
 route-map              Specify a route-map to be applied for filtering routes received
                        from or sent to the peer.
 route-reflector-cl... Act as a route reflector for the peer.
 route-refresh          Enable or disable the advertisement of route-refresh capability in
                        the Open message sent to the peer.
 send-community         Enable or disable sending the community attribute in route updates
                        to the peer.
 shutdown               Shutdown the BGP peering session without removing the associated
                        peer configuration.
 timers                 Configure the keepalive and hold-time values for the peer.
 ttl-security           Configure the TTL security for this peer.
 update-source          Specify the source address to accept TCP connections from the
                        peer.
 use-med                Enable or disable the comparison of MED attribute for the same
                        route received from two different autonomous systems.
 weight                 Specify the weight for all routes received from the specified
                        peer.


ArubaOS-Switch(bgp)# neighbor 10.0.101.31 remote-as 64503 ?
 <cr>

ArubaOS-Switch(bgp)# neighbor 10.0.101.31 remote-as 64503


ArubaOS-Switch(bgp)# neighbor 10.0.101.41 remote-as 64504


ArubaOS-Switch(bgp)# neighbor 10.0.101.51 remote-as 64505


ArubaOS-Switch(bgp)# redistribute connected


ArubaOS-Switch(bgp)# redistribute static


ArubaOS-Switch(bgp)# enable


ArubaOS-Switch(bgp)# network 10.0.221.0/24


ArubaOS-Switch# show ip bgp ?
 as-path                Shows list of unique as-paths learnt by this router.
 community              Show routes belonging to the specified communities.
 general                Show a global configuration details.
 IP-ADDR/MASK-LENGTH    Show routes matching this network ipv4 address.
 neighbor               Show information about the state of BGP peering session<ip-addr> -
                        Show information only for this peer.
 redistribute           Show protocols being redistributed into BGP.
 regexp                 Show BGP routes whose as-path information matches the supplied
                        regular expression.
 route                  Displays as-path or community information of the BGP routes.
 summary                Show a summary of BGP peer state information.
 <cr>
```

```
ArubaOS-Switch# show ip bgp summary

 Peer Information

  Remote Address  Remote-AS Local-AS State         Admin Status
  --------------- --------- -------- ------------- ------------
  10.0.101.31     64503     64502    Established   Start
  10.0.101.41     64504     64502    Established   Start
  10.0.101.51     64505     64502    Established   Start
```

Comware5

```
[Comware5]bgp ?
  INTEGER<1-4294967295>  Autonomous system number

[Comware5]bgp 64503 ?
  <cr>

[Comware5]bgp 64503


[Comware5-bgp]?
Bgp protocol view commands:
  aggregate                 Configure BGP aggregate entries
  balance                   Set maximum number of balanced paths
  bestroute                 Change the default best route selection
  cfd                       Connectivity fault detection (IEEE 802.1ag)
  compare-different-as-med  Allow comparing MED from different AS
  confederation             AS confederation parameters
  dampening                 Enable route-flap dampening
  default                   Set default value for BGP
  default-route             Default route operation
  display                   Display current system information
  ebgp-interface-sensitive  Immediately reset session if a link connected peer
                            goes down
  filter-policy             Filter networks in routing updates
  graceful-restart          Graceful Restart capability
  group                     Create a peer group
  ignore-first-as           Ignore first-as checking for EBGP routes
  import-route              Import route information from another routing
                            protocol
  ipv4-family               Specify IPv4 address family
  ipv6-family               IPv6 address family
  log-peer-change           Log any session status and event change information
  mtracert                  Trace route to multicast source
  network                   Specify a network to announce via BGP
  peer                      Specify a peer router
  ping                      Ping function
  preference                Define an administrative preference
  quit                      Exit from current command view
  reflect                   Configure client to client route reflection
  reflector                 Specify reflector to configure client to client
                            route reflection
  return                    Exit to User View
  router-id                 Override configured router identifier
  save                      Save current configuration
  summary                   Summarize IGP routes to a natural network
  synchronization           Perform IGP synchronization
  timer                     Configure timers for BGP
  tracert                   Trace route function
  undo                      Cancel current setting
```

```
[Comware5-bgp]router-id 10.0.0.3


[Comware5-bgp]peer ?
  STRING<1-47>  Specify a peer group
  X.X.X.X       Specify an IPv4 peer address

[Comware5-bgp]peer 10.0.101.21 ?
  advertise-community      Send community attribute to this peer
  advertise-ext-community  Advertise extended community
  allow-as-loop            Configure permit of as-path loop
  as-number                AS number
  as-path-acl              Set the filter list of peer or peer group
  bfd                      Enable BFD for this peer
  capability-advertise     Advertise capability
  connect-interface        Set interface name to be used as session's output
                           interface
  default-route-advertise  Advertise default route to this peer
  description              Configure description information about peer
  dscp                     Differentiated Services Codepoint (DSCP)
  ebgp-max-hop             EBGP Multihop
  enable                   Enable peer
  fake-as                  Configure a fake AS number for the peer
  filter-policy            BGP filter list
  group                    Specify a peer group
  ignore                   Suspend the peer session for this peer
  ip-prefix                Specify BGP route filtering policy based on
                           ip-prefix
  keep-all-routes          Keep all original routes' information from the peer
  log-change               Log any session status and event change information
  next-hop-local           Specify local address as the next hop of routes
                           advertised to the peer
  password                 Peer password
  preferred-value          Set route PrefVal to this peer
  public-as-only           Remove private AS number from outbound updates
  reflect-client           Configure a peer as a route reflector client
  route-limit              Number of routes limited from this peer
  route-policy             Apply route-policy
  route-update-interval    Route update interval
  substitute-as            Substitute with local AS
  timer                    Configure timers for a peer

[Comware5-bgp]peer 10.0.101.21 as-number 64502 ?
  <cr>

[Comware5-bgp]peer 10.0.101.21 as-number 64502


[Comware5-bgp]import-route direct


[Comware5-bgp]network 10.0.231.0 24


[Comware5]display bgp ?
  group          Peer groups
  ipv6           IPv6 address family
  multicast      Multicast address family
  network        Routes advertised through network command
  paths          Path attribute information
  peer           Specify a peer router
  routing-table  Display BGP routes
  vpnv4          VPNv4 address family
```

```
  vpnv6          VPNv6 address family

Comware5]display bgp peer

 BGP local router ID : 10.0.0.3
 Local AS number : 64503
 Total number of peers : 1                 Peers in established state : 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  10.0.101.21          64502       96       96    0       3 01:32:32 Established
```

Comware7

```
[Comware7]bgp ?
  INTEGER<1-4294967295>  Autonomous system number

[Comware7]bgp 64503 ?
  <cr>

[Comware7]bgp 64503


[Comware7-bgp]?
Bgp protocol view commands:
  address-family            Specify an address family
  advertise-rib-active      Advertise the best route in IP routing table
  bgp                       BGP specific commands
  cfd                       Connectivity Fault Detection (CFD) module
  confederation             Configure AS confederation parameters
  diagnostic-logfile        Diagnostic log file configuration
  display                   Display current system information
  ebgp-interface-sensitive  Immediately reset session if a link connected peer
                            goes down
  graceful-restart          Configure Graceful Restart (GR) capability
  group                     Create a peer group
  ignore-first-as           Ignore the first AS number of eBGP route updates
  ip                        Specify Internet Protocol (IP) configuration
                            information
  log-peer-change           Log any session status and event change information
  logfile                   Log file configuration
  monitor                   System monitor
  non-stop-routing          Enable NSR
  peer                      Specify BGP peers
  ping                      Ping function
  primary-path-detect       Enable primary path detect function
  quit                      Exit from current command view
  return                    Exit to User View
  router-id                 Configure router ID
  save                      Save current configuration
  security-logfile          Security log file configuration
  timer                     Configure timers for BGP
  tracert                   Tracert function
  undo                      Cancel current setting
  vpn                       Set forwarding mode of MPLS L3VPN on egress PE


[Comware7-bgp]router-id 10.0.0.5


[Comware7-bgp]peer ?
  STRING<1-47>  Specify a peer group by its name
  X.X.X.X       IPv4 address
  X:X::X:X      IPv6 address
```

```
[Comware7-bgp]peer 10.0.101.21 ?
  INTEGER<0-32>          Specify a Mask length of IPv4 address
  as-number              AS number
  bfd                    Enable BFD for the peers
  capability-advertise   Advertise capability
  connect-interface      Set interface name to be used as session's output
                         interface
  description            Configure description information about the peers
  ebgp-max-hop           EBGP Multihop
  fake-as                Configure a fake AS number for the peers
  group                  Specify a peer-group
  ignore                 Disable session establishment with the peers
  ignore-originatorid    Ignore the originator ID attribute in received BGP
                         routes
  low-memory-exempt      Exempt the EBGP peers from low-memory shutdown
  password               Specify a password
  route-update-interval  Specify the interval for sending the same update to the
                         peers
  substitute-as          Replace the AS number in the AS_PATH attribute with the
                         local
  timer                  Configure timers for the peers
  ttl-security           Configure the Generalized TTL Security Mechanism (GTSM)

[Comware7-bgp]peer 10.0.101.21 as-number 64502 ?
  <cr>

[Comware7-bgp]peer 10.0.101.21 as-number 64502


[Comware7-bgp]address-family ?
  ipv4   Specify the IPv4 address family
  ipv6   Specify the IPv6 address family
  l2vpn  Specify the L2VPN address family
  vpnv4  Specify the VPNv4 address family
  vpnv6  Specify the VPNv6 address family

[Comware7-bgp]address-family ipv4 ?
  unicast  Specify the unicast address family
  <cr>

[Comware7-bgp]address-family ipv4 unicast ?
  <cr>

[Comware7-bgp]address-family ipv4 unicast

[Comware7-bgp-ipv4]?
Bgp-ipv4 protocol view commands:
  aggregate                 Create a summary route
  balance                   Configure BGP load balancing
  bestroute                 Change the default best route selection
  cfd                       Connectivity Fault Detection (CFD) module
  compare-different-as-med  Compare the MEDs of routes from different ASs
  dampening                 Enable route-flap dampening
  default                   Set default value for BGP
  default-route             Default route operation
  diagnostic-logfile        Diagnostic log file configuration
  display                   Display current system information
  fast-reroute              Configure fast reroute
  filter-policy             Filter networks in route updates
  import-route              Import routes from another routing protocol
  logfile                   Log file configuration
  monitor                   System monitor
```

```
  network                    Specify a network to advertise via BGP
  peer                       Specify BGP peers
  pic                        Enable Prefix Independent Convergence (PIC)
  ping                       Ping function
  preference                 Configure the preference of BGP routes
  quit                       Exit from current command view
  reflect                    Configure route reflection
  reflector                  Configure the route reflector
  return                     Exit to User View
  save                       Save current configuration
  security-logfile           Security log file configuration
  summary                    Summarize subnet routes to classful network routes
  tracert                    Tracert function
  undo                       Cancel current setting

[Comware7-bgp-ipv4]peer 10.0.101.21 ?
  INTEGER<0-32>             Specify a Mask length of IPv4 address
  advertise-community       Send community attribute to the peers
  advertise-ext-community   Advertise extended community
  allow-as-loop             Configure permit of as-path loop
  as-path-acl               Specify an AS path ACL
  default-route-advertise   Advertise default route to the peers
  enable                    Enable the specified peers
  filter-policy             Filter networks in route updates
  keep-all-routes           Save original routing information from the peers
  label-route-capability    Send labeled route to the peers
  next-hop-local            Specify local address as the next hop of routes
                            advertised to the peers
  preferred-value           Assign a preferred value to routes received from the
                            peers
  prefix-list               Specify BGP route filtering policy based on a prefix
                            list
  public-as-only            Do not keep private AS numbers in BGP updates
  reflect-client            Configure the peers as route reflectors
  route-limit               Configure the maximum number of routes that can be
                            received from the peers
  route-policy              Specify a routing policy

[Comware7-bgp-ipv4]peer 10.0.101.21 enable ?
  <cr>

[Comware7-bgp-ipv4]peer 10.0.101.21 enable


[Comware7-bgp-ipv4]import-route direct


[Comware7-bgp-ipv4]network 10.0.251.0 24


[Comware7]display bgp ?
  dampening         BGP dampening information
  group             Display peer group information
  l2vpn             Specify the L2VPN address family
  network           Routing information advertised with the network command or
                    short-cut route information
  non-stop-routing  Display BGP NSR information
  paths             Path attribute information
  peer              Display peer information
  routing-table     Display BGP routes
  update-group      Display update group information

[Comware7]display bgp peer ?
```

```
  ipv4   Specify the IPv4 address family
  ipv6   Specify the IPv6 address family
  l2vpn  Specify the L2VPN address family
  vpnv4  Specify the VPNv4 address family
  vpnv6  Specify the VPNv6 address family

[Comware7]display bgp peer ipv4 ?
  >             Redirect it to a file
  >>            Redirect it to a file in append mode
  X.X.X.X       IPv4 address
  group-name    Specify a peer group by its name
  standby       Display information on the standby process
  unicast       Specify the unicast address family
  verbose       Detailed information
  vpn-instance  Specify a VPN instance
  |             Matching output
  <cr>

[Comware7]display bgp peer ipv4

 BGP local router ID: 10.0.0.5
 Local AS number: 64505
 Total number of peers: 1                 Peers in established state: 1

  * - Dynamically created peer
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  10.0.101.21          64502       78       80    0       3 01:10:44 Established
```

Cisco

```
Cisco(config)#router bgp ?
  <1-4294967295>  Autonomous system number
  <1.0-XX.YY>     Autonomous system number

Cisco(config)#router bgp 64504 ?
  <cr>

Cisco(config)#router bgp 64504


Cisco(config-router)#bgp ?
  aggregate-timer         Configure Aggregation Timer
  always-compare-med      Allow comparing MED from different neighbors
  asnotation              Change the default asplain notation
  bestpath                Change the default bestpath selection
  client-to-client        Configure client to client route reflection
  cluster-id              Configure Route-Reflector Cluster-id (peers may
                          reset)
  confederation           AS confederation parameters
  dampening               Enable route-flap dampening
  default                 Configure BGP defaults
  deterministic-med       Pick the best-MED path among paths advertised from
                          the neighboring AS
  dmzlink-bw              Use DMZ Link Bandwidth as weight for BGP multipaths
  enforce-first-as        Enforce the first AS for EBGP routes(default)
  fast-external-fallover  Immediately reset session if a link to a directly
                          connected external peer goes down
  graceful-restart        Graceful restart capability parameters
  inject-map              Routemap which specifies prefixes to inject
  log-neighbor-changes    Log neighbor up/down and reset reason
  maxas-limit             Allow AS-PATH attribute from any neighbor imposing a
                          limit on number of ASes
  nexthop                 Nexthop tracking commands
```

```
  nopeerup-delay          Set how long BGP will wait for the first peer to come
                          up before beginning the update delay or graceful
                          restart timers (in seconds)
  redistribute-internal   Allow redistribution of iBGP into IGPs (dangerous)
  regexp                  Select regular expression engine
  route-map               route-map control commands
  router-id               Override configured router identifier (peers will
                          reset)
  scan-time               Configure background scanner interval
  slow-peer               Configure slow-peer
  soft-reconfig-backup    Use soft-reconfiguration inbound only when
                          route-refresh is not negotiated
  suppress-inactive       Suppress routes that are not in the routing table
  transport               global enable/disable transport session parameters
  update-delay            Set the max initial delay for sending update
  upgrade-cli             Upgrade to hierarchical AFI mode

Cisco(config-router)#bgp router-id ?
  A.B.C.D  Manually configured router identifier
  vrf      vrf-specific router id configuration

Cisco(config-router)#bgp router-id 10.0.0.4 ?
  <cr>

Cisco(config-router)#bgp router-id 10.0.0.4


Cisco(config-router)#?
Router configuration commands:
  address-family       Enter Address Family command mode
  aggregate-address    Configure BGP aggregate entries
  auto-summary         Enable automatic network number summarization
  bgp                  BGP specific commands
  default              Set a command to its defaults
  default-information  Control distribution of default information
  default-metric       Set metric of redistributed routes
  distance             Define an administrative distance
  distribute-list      Filter networks in routing updates
  exit                 Exit from routing protocol configuration mode
  help                 Description of the interactive help system
  maximum-paths        Forward packets over multiple paths
  neighbor             Specify a neighbor router
  network              Specify a network to announce via BGP
  no                   Negate a command or set its defaults
  redistribute         Redistribute information from another routing protocol
  scope                Enter scope command mode
  synchronization      Perform IGP synchronization
  table-map            Map external entry attributes into routing table
  template             Enter template command mode
  timers               Adjust routing timers

Cisco(config-router)#neighbor ?
  A.B.C.D     Neighbor address
  WORD        Neighbor tag
  X:X:X:X::X  Neighbor IPv6 address

Cisco(config-router)#neighbor 10.0.101.21 ?
  activate                 Enable the Address Family for this Neighbor
  advertise-map            specify route-map for conditional advertisement
  advertisement-interval   Minimum interval between sending BGP routing updates
  allowas-in               Accept as-path with my AS present in it
  capability               Advertise capability to the peer
  default-originate        Originate default route to this neighbor
```

```
  description               Neighbor specific description
  disable-connected-check   one-hop away EBGP peer using loopback address
  distribute-list           Filter updates to/from this neighbor
  dmzlink-bw                Propagate the DMZ link bandwidth
  ebgp-multihop             Allow EBGP neighbors not on directly connected
                            networks
  fall-over                 session fall on peer route lost
  filter-list               Establish BGP filters
  ha-mode                   high availability mode
  inherit                   Inherit a template
  local-as                  Specify a local-as number
  maximum-prefix            Maximum number of prefixes accepted from this peer
  next-hop-self             Disable the next hop calculation for this neighbor
  next-hop-unchanged        Propagate next hop unchanged for iBGP paths to this
                            neighbor
  password                  Set a password
  peer-group                Member of the peer-group
  prefix-list               Filter updates to/from this neighbor
  remote-as                 Specify a BGP neighbor
  remove-private-as         Remove private AS number from outbound updates
  route-map                 Apply route map to neighbor
  route-reflector-client    Configure a neighbor as Route Reflector client
  send-community            Send Community attribute to this neighbor
  shutdown                  Administratively shut down this neighbor
  slow-peer                 Configure slow-peer
  soft-reconfiguration      Per neighbor soft reconfiguration
  soo                       Site-of-Origin extended community
  timers                    BGP per neighbor timers
  translate-update          Translate Update to MBGP format
  transport                 Transport options
  ttl-security              BGP ttl security check
  unsuppress-map            Route-map to selectively unsuppress suppressed
                            routes
  update-source             Source of routing updates
  version                   Set the BGP version to match a neighbor
  weight                    Set default weight for routes from this neighbor

Cisco(config-router)#neighbor 10.0.101.21 remote-as ?
  <1-4294967295>  AS of remote neighbor
  <1.0-XX.YY>     AS of remote neighbor

Cisco(config-router)#neighbor 10.0.101.21 remote-as 64502 ?
  shutdown  Administratively shut down this neighbor
  <cr>

Cisco(config-router)#neighbor 10.0.101.21 remote-as 64502


Cisco(config-router)#redistribute connected


Cisco(config-router)#network 10.0.241.0 ?
  backdoor   Specify a BGP backdoor route
  mask       Network mask
  nlri       Specify nlri type for network
  route-map  Route-map to modify the attributes
  <cr>

Cisco(config-router)#network 10.0.241.0 mask ?
  A.B.C.D  Network mask

Cisco(config-router)#network 10.0.241.0 mask 255.255.255.0
```

```
Cisco#show ip bgp ?
  A.B.C.D             Network in the BGP routing table to display
  A.B.C.D/nn          IP prefix <network>/<length>, e.g., 35.0.0.0/8
  all                 All address families
  cidr-only           Display only routes with non-natural netmasks
  community           Display routes matching the communities
  community-list      Display routes matching the community-list
  dampening           Display detailed information about dampening
  extcommunity-list   Display routes matching the extcommunity-list
  filter-list         Display routes conforming to the filter-list
  import              Display route topology import / export activity
  inconsistent-as     Display only routes with inconsistent origin ASs
  injected-paths      Display all injected paths
  ipv4                Address family
  ipv6                Address family
  l2vpn               Address family
  labels              Display Labels for IPv4 NLRI specific information
  neighbors           Detailed information on TCP and BGP neighbor connections
  nexthops            Nexthop address table
  nsap                Address family
  oer-paths           Display all oer controlled paths
  paths               Path information
  peer-group          Display information on peer-groups
  pending-prefixes    Display prefixes pending deletion
  prefix-list         Display routes matching the prefix-list
  quote-regexp        Display routes matching the AS path "regular expression"
  regexp              Display routes matching the AS path regular expression
  replication         Display replication status of update-group(s)
  rib-failure         Display bgp routes that failed to install in the routing
                      table (RIB)
  route-map           Display routes matching the route-map
  summary             Summary of BGP neighbor status
  template            Display peer-policy/peer-session templates
  topology            Routing topology instance
  update-group        Display information on update-groups
  update-sources      Update source interface table
  version             Display prefixes with matching version numbers
  vpnv4               Address family
  vpnv6               Address family
  |                   Output modifiers

Cisco#show ip bgp summary
BGP router identifier 10.0.0.4, local AS number 64504
BGP table version is 5, main routing table version 5
4 network entries using 544 bytes of memory
4 path entries using 208 bytes of memory
4/4 BGP path/bestpath attribute entries using 496 bytes of memory
3 BGP AS-PATH entries using 72 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1320 total bytes of memory
BGP activity 4/0 prefixes, 4/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.101.21     4        64502       8       8        5    0    0 00:03:23        3
```

b) iBGP

ArubaOS-Switch	Comware5	Cisco
iBGP router:	iBGP router:	iBGP router:

ArubaOS-Switch-2(config)# router bgp 64502	[Comware5-2]bgp 64503	Cisco-2(config)#router bgp 64504
ArubaOS-Switch-2(bgp)# bgp router-id 10.0.0.12	[Comware5-2-bgp]router-id 10.0.0.13	Cisco-2(config-router)#bgp router-id 10.0.0.14
ArubaOS-Switch-2(bgp)# neighbor 10.0.112.254 remote-as 64502	[Comware5-2-bgp]peer 10.0.113.254 as-number 64503	Cisco-2(config-router)#neighbor 10.0.114.254 remote-as 64504
ArubaOS-Switch-2(bgp)# redistribute connected	[Comware5-2-bgp]import-route direct	Cisco-2(config-router)#redistribute connected
ArubaOS-Switch-2(bgp)# enable		
ArubaOS-Switch-2(bgp)# network 10.0.222.0/24	[Comware5-2-bgp]network 10.0.232.0 24	Cisco-2(config-router)#network 10.0.242.0 mask 255.255.255.0
ArubaOS-Switch-2# show ip bgp summary	[Comware5-2-bgp]display bgp peer	Cisco-2#show ip bgp summary
eBGP router additional commands after section "a" has been completed.	eBGP router additional commands after section "a" has been completed.	eBGP router additional commands after section "a" has been completed.
ArubaOS-Switch(config)# router bgp 64502	[Comware5]bgp 64503	Cisco(config)#router bgp 64504
ArubaOS-Switch(bgp)# neighbor 10.0.112.1 remote-as 64502	[Comware5-bgp]peer 10.0.113.1 as-number 64503	Cisco(config-router)#neighbor 10.0.114.1 remote-as 64504
ArubaOS-Switch(bgp)# neighbor 10.0.112.1 next-hop-self	[Comware5-bgp]peer 10.0.113.1 next-hop-local	Cisco(config-router)#neighbor 10.0.114.1 next-hop-self
ArubaOS-Switch# show ip bgp summary	[Comware5]display bgp peer	Cisco#show ip bgp summary
	Comware7	
	iBGP router:	
	[Comware7-2]bgp 64505	
	[Comware7-2-bgp]router-id 10.0.0.15	
	[Comware7-2-bgp]peer 10.0.115.254 as-number 64505	
	[Comware7-2-bgp]address-family ipv4 unicast	
	[Comware7-2-bgp-ipv4]peer 10.0.115.254 enable	
	[Comware7-2-bgp-ipv4]import-route direct	
	[Comware7-bgp-ipv4]network 10.0.252.0 24	
	[Comware7-2]display bgp peer ipv4	
	eBGP router additional commands after section "a" has been completed.	
	[Comware7]bgp 64505	
	[Comware7-bgp]peer 10.0.115.1 as-number 64505	

	[Comware7-bgp]address-family ipv4 unicast	
	[Comware7-bgp-ipv4]peer 10.0.115.1 enable	
	[Comware7-bgp-ipv4]peer 10.0.115.1 next-hop-local	
	[Comware7-2]display bgp peer ipv4	

ArubaOS-Switch

iBGP router: (basically the same steps as for eBGP router configuration)

```
ArubaOS-Switch-2(config)# router bgp 64502

ArubaOS-Switch-2(bgp)# bgp router-id 10.0.0.12

ArubaOS-Switch-2(bgp)# neighbor 10.0.112.254 remote-as 64502

ArubaOS-Switch-2(bgp)# enable

ArubaOS-Switch-2(bgp)# redistribute connected

ArubaOS-Switch-2(bgp)# network 10.0.222.0/24


ArubaOS-Switch-2# show ip bgp summary

 Peer Information

  Remote Address  Remote-AS Local-AS State         Admin Status
  --------------- --------- -------- ------------- ------------
  10.0.112.254    64502     64502    Established   Start
```

eBGP router additional commands after section “a” has been completed.

```
ArubaOS-Switch(config)# router bgp 64502

ArubaOS-Switch(bgp)# neighbor 10.0.112.1 remote-as 64502

ArubaOS-Switch(bgp)# neighbor 10.0.112.1 next-hop-self


ArubaOS-Switch# show ip bgp summary

 Peer Information

  Remote Address  Remote-AS Local-AS State         Admin Status
  --------------- --------- -------- ------------- ------------
  10.0.101.31     64503     64502    Established   Start
  10.0.101.41     64504     64502    Established   Start
  10.0.101.51     64505     64502    Established   Start
  10.0.112.1      64502     64502    Established   Start
```

Comware5

iBGP router: (basically the same steps as for eBGP router configuration)

```
[Comware5-2]bgp 64503

[Comware5-2-bgp]router-id 10.0.0.13

[Comware5-2-bgp]peer 10.0.113.254 as-number 64503

[Comware5-2-bgp]network 10.0.232.0 24

[Comware5-2-bgp]import-route direct


[Comware5-2]display bgp peer

 BGP local router ID : 10.0.0.13
 Local AS number : 64503
 Total number of peers : 1                 Peers in established state : 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  10.0.113.254         64503      170      144    0      21 02:28:17 Established
```

eBGP router additional commands after section "a" has been completed.

```
[Comware5]bgp 64503

[Comware5-bgp]peer 10.0.113.1 as-number 64503

[Comware5-bgp]peer 10.0.113.1 next-hop-local


[Comware5]display bgp peer

 BGP local router ID : 10.0.0.3
 Local AS number : 64503
 Total number of peers : 2                 Peers in established state : 2

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  10.0.101.21          64502      209      191    0      18 03:02:46 Established
  10.0.113.1           64503      144      171    0       3 02:28:58 Established
```

Comware7

iBGP router: (basically the same steps as for eBGP router configuration)

```
[Comware7-2]bgp 64505

[Comware7-2-bgp]router-id 10.0.0.15

[Comware7-2-bgp]peer 10.0.115.254 as-number 64505

[Comware7-2-bgp]address-family ipv4 unicast

[Comware7-2-bgp-ipv4]peer 10.0.115.254 enable

[Comware7-2-bgp-ipv4]import-route direct

[Comware7-2-bgp-ipv4]network 10.0.252.0 24
```

```
[Comware7-2]display bgp peer ipv4

 BGP local router ID: 10.0.0.15
 Local AS number: 64505
 Total number of peers: 1                 Peers in established state: 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  10.0.115.254         64505       29       25    0      21 00:15:17 Established
```

eBGP router additional commands after section "a" has been completed.

```
[Comware7]bgp 64505

[Comware7-bgp]peer 10.0.115.1 as-number 64505

[Comware7-bgp]address-family ipv4 unicast

[Comware7-bgp-ipv4]peer 10.0.115.1 enable

[Comware7-bgp-ipv4]peer 10.0.115.1 next-hop-local


[Comware7]display bgp peer

 BGP local router ID: 10.0.0.5
 Local AS number: 64505
 Total number of peers: 2                 Peers in established state: 2

  * - Dynamically created peer
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  10.0.101.21          64502      214      209    0      18 03:00:37 Established
  10.0.115.1           64505       25       31    0       3 00:16:56 Established
```

Cisco

iBGP router: (basically the same steps as for eBGP router configuration)

```
Cisco-2(config)#router bgp 64504

Cisco-2(config-router)#bgp router-id 10.0.0.14

Cisco-2(config-router)#neighbor 10.0.114.254 remote-as 64504

Cisco-2(config-router)#redistribute connected

Cisco-2(config-router)#network 10.0.242.0 mask 255.255.255.0


Cisco-2#show ip bgp summary
BGP router identifier 10.0.0.14, local AS number 64504
BGP table version is 26, main routing table version 26
23 network entries using 2691 bytes of memory
24 path entries using 1248 bytes of memory
11/10 BGP path/bestpath attribute entries using 1540 bytes of memory
3 BGP AS-PATH entries using 72 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
```

```
BGP using 5551 total bytes of memory
BGP activity 24/1 prefixes, 25/1 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.114.254    4 64504      86      72       26    0    0 01:06:14       21
```

eBGP router additional commands after section "a" has been completed.

```
Cisco(config)#router bgp 64504

Cisco(config-router)#neighbor 10.0.114.1 remote-as 64504

Cisco(config-router)#neighbor 10.0.114.1 next-hop-self


Cisco#show ip bgp summary
BGP router identifier 10.0.0.4, local AS number 64504
BGP table version is 47, main routing table version 47
23 network entries using 3128 bytes of memory
25 path entries using 1300 bytes of memory
10/10 BGP path/bestpath attribute entries using 1240 bytes of memory
3 BGP AS-PATH entries using 72 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 5740 total bytes of memory
BGP activity 26/3 prefixes, 36/11 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.101.21     4        64502     197     198       47    0    0 02:50:50       18
10.0.114.1      4        64504      73      87       47    0    0 01:07:00        3
```

Chapter 27 VRRP

This chapter compares the commands used to configure Virtual Router Redundancy Protocol (VRRP). Cisco also supports Hot Standby Router Protocol (HSRP), which is not compatible with VRRP.

In many networks, edge devices are often configured to send packets to a statically configured default router. If this router becomes unavailable, the devices that use it as their first-hop router become isolated from the network. VRRP, which is based on RFC 5798, uses dynamic failover to ensure the availability of an end node's default router. This is done by assigning the IP address used as the default route to a "virtual router," or VR.

On a given VLAN, a VR includes two or more member routers that you configure with a virtual IP address that is the default gateway's IP address. The VR includes an owner router assigned to forward traffic designated for the virtual router (If the owner is forwarding traffic for the VR, it is the master router for that VR) and one or more prioritized backup routers (If a backup is forwarding traffic for the VR, it has replaced the owner as the master router for that VR.)

ArubaOS-Switch	Comware5	Cisco
ArubaOS-Switch(config)# router vrrp ArubaOS-Switch(vrrp)# ipv4 enable		
ArubaOS-Switch(vrrp)# vlan 220	[Comware5]interface vlan 220	Cisco(config)#interface vlan 100
ArubaOS-Switch(vlan-220)# vrrp vrid 220 ArubaOS-Switch(vlan-220-vrid-220)# virtual-ip-address 10.1.220.1	[Comware5-Vlan-interface220]vrrp vrid 220 virtual-ip 10.1.220.1	Cisco(config-if)#vrrp 100 ip 10.1.100.1
ArubaOS-Switch(vlan-220-vrid-220)# priority 254	[Comware5-Vlan-interface220]vrrp vrid 220 priority 100	Cisco(config-if)#vrrp 100 priority 100
ArubaOS-Switch(vlan-220-vrid-220)# enable		
	[Comware5-Vlan-interface220]vrrp version 2	
ArubaOS-Switch# show vrrp	[Comware5]display vrrp verbose	Cisco#show vrrp
	[Comware5]display vrrp	Cisco#show vrrp brief
ArubaOS-Switch# show vrrp vlan 220	[Comware5]display vrrp interface Vlan-interface 220	Cisco#show vrrp interface vlan 100
	Comware7	
	[Comware7]interface Vlan-interface 100	
	[Comware7-Vlan-interface100]vrrp vrid 100 virtual-ip 10.1.100.1	
	[Comware7-Vlan-interface100]vrrp vrid 100 priority 254	

	[Comware7-Vlan-interface100]vrrp version 2	
	[Comware7]display vrrp verbose	
	[Comware7]display vrrp	
	[Comware7]display vrrp interface vlan 100 verbose	

ArubaOS-Switch

```
ArubaOS-Switch(config)# router vrrp

ArubaOS-Switch(vrrp)# ?
 ipv4                   Configure VRRP for IPv4 virtual routers.
 ipv6                   Configure VRRP for IPv6 virtual routers.
 traps                  Enable/disable sending SNMP traps for the following situations: o
                        'New Master' - Sent when the switch transitions to the 'Master'
                        state.
 virtual-ip-ping        If disabled, globally prevents a response to ping requests to the
                        virtual router IP addresses configured on all backup routers.

ArubaOS-Switch(vrrp)# ipv4 ?
 disable                Disable VRRP globally.
 enable                 Enable VRRP globally.

ArubaOS-Switch(vrrp)# ipv4 enable


ArubaOS-Switch(vrrp)# vlan 220

ArubaOS-Switch(vlan-220)# vrrp vrid 220

ArubaOS-Switch(vlan-220-vrid-220)# virtual-ip-address 10.1.220.1

ArubaOS-Switch(vlan-220-vrid-220)# priority 254

ArubaOS-Switch(vlan-220-vrid-220)# enable


ArubaOS-Switch# show vrrp

 VRRP Global Statistics Information

  VRRP Enabled            : Yes
  Invalid VRID Pkts Rx    : 0
  Checksum Error Pkts Rx  : 0
  Bad Version Pkts Rx     : 0
  Virtual Routers Respond To Ping Requests : No


 VRRP Virtual Router Statistics Information

  Vlan ID                   : 220
  Virtual Router ID         : 220
  Protocol Version          : 2
  State                     : Master
  Up Time                   : 10 mins
  Virtual MAC Address       : 00005e-0001dc
  Master's IP Address       : 10.1.220.10
  Associated IP Addr Count  : 1          Near Failovers            : 0
```

```
  Advertise Pkts Rx        : 13          Become Master             : 2
  Zero Priority Rx         : 0           Zero Priority Tx          : 0
  Bad Length Pkts          : 0           Bad Type Pkts             : 0
  Mismatched Interval Pkts : 0           Mismatched Addr List Pkts : 0
  Mismatched IP TTL Pkts   : 0           Mismatched Auth Type Pkts : 0


ArubaOS-Switch# show vrrp vlan 220

 VRRP Virtual Router Statistics Information

  Vlan ID                  : 220
  Virtual Router ID        : 220
  Protocol Version         : 2
  State                    : Master
  Up Time                  : 12 mins
  Virtual MAC Address      : 00005e-0001dc
  Master's IP Address      : 10.1.220.10
  Associated IP Addr Count : 1           Near Failovers            : 0
  Advertise Pkts Rx        : 13          Become Master             : 2
  Zero Priority Rx         : 0           Zero Priority Tx          : 0
  Bad Length Pkts          : 0           Bad Type Pkts             : 0
  Mismatched Interval Pkts : 0           Mismatched Addr List Pkts : 0
  Mismatched IP TTL Pkts   : 0           Mismatched Auth Type Pkts : 0
```

Comware5

```
[Comware5]interface vlan 220

[Comware5-Vlan-interface220]vrrp ?
  dot1q     IEEE 802.1Q encapsulation
  ipv6      Specify IPv6 Virtual Router
  un-check  Uncheck VRRP packet TTL value
  version   Specify a VRRP version
  vrid      Specify Virtual Router Identifier

[Comware5-Vlan-interface220]vrrp vrid ?
  INTEGER<1-255>  Virtual Router Identifier

[Comware5-Vlan-interface220]vrrp vrid 220 ?
  authentication-mode  Specify password and authentication mode
  preempt-mode         Specify preempt mode
  priority             Specify priority
  timer                Specify timer
  track                Specify object tracked
  virtual-ip           Specify virtual IP address
  weight               Specify VRRP weight track function

[Comware5-Vlan-interface220]vrrp vrid 220 virtual-ip 10.1.220.1


[Comware5-Vlan-interface220]vrrp vrid 220 priority ?
  INTEGER<1-254>  The level of priority

[Comware5-Vlan-interface220]vrrp vrid 220 priority 100


[Comware5-Vlan-interface220]vrrp version ?
  INTEGER<2-3>  Version number

[Comware5-Vlan-interface220]vrrp version 2


[Comware5]display vrrp verbose
```

```
IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface220
     VRID           : 220             Adver Timer : 1
     Admin Status   : Up              State       : Backup
     Config Pri     : 100             Running Pri : 100
     Preempt Mode   : Yes             Delay Time  : 0
     Become Master  : 3450ms left
     Auth Type      : None
     Virtual IP     : 10.1.220.1
     Master IP      : 10.1.220.10


[Comware5]display vrrp
IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
 Interface          VRID   State       Run     Adver   Auth     Virtual
                                        Pri     Timer   Type        IP
 --------------------------------------------------------------------
 Vlan220            220    Backup      100     1       None     10.1.220.1


[Comware5]display vrrp interface Vlan-interface 220
IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers on interface Vlan220 : 1
 Interface          VRID   State       Run     Adver   Auth     Virtual
                                        Pri     Timer   Type        IP
 --------------------------------------------------------------------
 Vlan220            220    Backup      100     1       None     10.1.220.1
```

Comware7

```
[Comware7]interface Vlan-interface 100

[Comware7-Vlan-interface100]vrrp ?
  check-ttl  Enable TTL check on VRRP packets
  dot1q      Specify a VRRP control VLAN
  ipv6       Specify IPv6 Virtual Router
  version    Specify version of VRRP
  vrid       Specify the virtual router by its identifier

[Comware7-Vlan-interface100]vrrp vrid ?
  INTEGER<1-255>  Virtual router identifier

[Comware7-Vlan-interface100]vrrp vrid 100 ?
  authentication-mode  Configure authentication mode and authentication key
  preempt-mode         Enable preemption on the router
  priority             Configure the priority of the router
  shutdown             Shut down the virtual router
  source-interface     Specify the source interface for the VRRP group
  timer                Configure the value of the timer
  track                Associate a track entry with the VRRP group to control
                       master switchover in the VRRP group according to the
                       state change of the track entry
  virtual-ip           Assign an virtual IP address to the virtual router

[Comware7-Vlan-interface100]vrrp vrid 100 virtual-ip 10.1.100.1 ?
  <cr>
```

```
[Comware7-Vlan-interface100]vrrp vrid 100 virtual-ip 10.1.100.1


[Comware7-Vlan-interface100]vrrp vrid 100 priority ?
  INTEGER<1-254>  Priority value

[Comware7-Vlan-interface100]vrrp vrid 100 priority 254


[Comware7-Vlan-interface100]vrrp ?
  check-ttl  Enable TTL check on VRRP packets
  dot1q      Specify a VRRP control VLAN
  ipv6       Specify IPv6 Virtual Router
  version    Specify version of VRRP
  vrid       Specify the virtual router by its identifier

[Comware7-Vlan-interface100]vrrp version ?
  INTEGER<2-3>  Version of VRRP

[Comware7-Vlan-interface100]vrrp version 2


[Comware7]display vrrp ?
  >           Redirect it to a file
  >>          Redirect it to a file in append mode
  interface   Specify the interface
  ipv6        Specify IPv6 Virtual Router
  statistics  VRRP statistics
  verbose     Verbose information
  |           Matching output
  <cr>

[Comware7]display vrrp verbose
IPv4 Virtual Router Information:
 Running mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface100
     VRID           : 100                 Adver Timer  : 100
     Admin Status   : Up                  State        : Master
     Config Pri     : 254                 Running Pri  : 254
     Preempt Mode   : Yes                 Delay Time   : 0
     Auth Type      : None
     Virtual IP     : 10.1.100.1
     Virtual MAC    : 0000-5e00-0164
     Master IP      : 10.1.100.5


[Comware7]display vrrp
IPv4 Virtual Router Information:
 Running mode      : Standard
 Total number of virtual routers : 1
 Interface          VRID  State        Running Adver   Auth     Virtual
                                       Pri     Timer   Type        IP
 --------------------------------------------------------------------
 Vlan100            100   Master       254     100     None     10.1.100.1


[Comware7]display vrrp interface Vlan-interface 100 verbose
IPv4 Virtual Router Information:
 Running mode      : Standard
 Total number of virtual routers on interface Vlan-interface100 : 1
   Interface Vlan-interface100
```

```
     VRID           : 100                  Adver Timer  : 100
     Admin Status   : Up                   State        : Master
     Config Pri     : 254                  Running Pri  : 254
     Preempt Mode   : Yes                  Delay Time   : 0
     Auth Type      : None
     Virtual IP     : 10.1.100.1
     Virtual MAC    : 0000-5e00-0164
     Master IP      : 10.1.100.5
```

Cisco

```
Cisco(config)#interface vlan 100

Cisco(config-if)#?
Interface configuration commands:
  aaa                     Authentication, Authorization and Accounting.
  arp                     Set arp type (arpa, probe, snap) or timeout or log
                          options
  bandwidth               Set bandwidth informational parameter
  bgp-policy              Apply policy propagated by bgp community string
  carrier-delay           Specify delay for interface transitions
  cdp                     CDP interface subcommands
  cts                     Configure Cisco Trusted Security
  dampening               Enable event dampening
  datalink                Interface Datalink commands
  default                 Set a command to its defaults
  delay                   Specify interface throughput delay
  description             Interface specific description
  eou                     EAPoUDP Interface Configuration Commands
  exit                    Exit from interface configuration mode
  flow-sampler            Attach flow sampler to the interface
  help                    Description of the interactive help system
  history                 Interface history histograms - 60 second, 60 minute
                          and 72 hour
  hold-queue              Set hold queue depth
  ip                      Interface Internet Protocol config commands
  link                    Configure Link
  load-interval           Specify interval for load calculation for an
                          interface
  logging                 Configure logging for interface
  loopback                Configure internal loopback on an interface
  macro                   Command macro
  max-reserved-bandwidth  Maximum Reservable Bandwidth on an Interface
  mka                     MACsec Key Agreement (MKA) interface configuration
  neighbor                interface neighbor configuration mode commands
  network-policy          Network Policy
  nmsp                    NMSP interface configuration
  no                      Negate a command or set its defaults
  ntp                     Configure NTP
  private-vlan            Configure private VLAN SVI interface settings
  rate-limit              Rate Limit
  routing                 Per-interface routing configuration
  service-policy          Configure CPL Service Policy
  shutdown                Shutdown the selected interface
  snmp                    Modify SNMP interface parameters
  source                  Get config from another source
  spanning-tree           Spanning Tree Subsystem
  standby                 HSRP interface configuration commands
  timeout                 Define timeout values for this interface
  topology                Configure routing topology on the interface
  traffic-shape           Enable Traffic Shaping on an Interface or
                          Sub-Interface
  vrrp                    VRRP Interface configuration commands
  vtp                     Enable VTP on this interface
```

```
Cisco(config-if)#vrrp ?
  <1-255>  Group number

Cisco(config-if)#vrrp 100 ?
  authentication  Authentication string
  description     Group specific description
  ip              Enable Virtual Router Redundancy Protocol (VRRP) for IP
  preempt         Enable preemption of lower priority Master
  priority        Priority of this VRRP group
  timers          Set the VRRP timers
  track           Event Tracking

Cisco(config-if)#vrrp 100 ip ?
  A.B.C.D  VRRP group IP address

Cisco(config-if)#vrrp 100 ip 10.1.100.1 ?
  secondary  Specify an additional VRRP address for this group
  <cr>

Cisco(config-if)#vrrp 100 ip 10.1.100.1


Cisco(config-if)#vrrp 100 priority ?
  <1-254>  Priority level

Cisco(config-if)#vrrp 100 priority 100 ?
  <cr>

Cisco(config-if)#vrrp 100 priority 100


Cisco#show vrrp ?
  all        Include groups in disabled state
  brief      Brief output
  interface  VRRP interface status and configuration
  |          Output modifiers
  <cr>


Cisco#show vrrp
Vlan100 - Group 100
  State is Backup
  Virtual IP address is 10.1.100.1
  Virtual MAC address is 0000.5e00.0164
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 101
  Master Router is 10.1.100.5, priority is 254
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.605 sec (expires in 3.043 sec)


Cisco#show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Vl100              100 101 3605       Y  Backup  10.1.100.5      10.1.100.1


Cisco#show vrrp interface vlan 100
Vlan100 - Group 100
  State is Backup
  Virtual IP address is 10.1.100.1
  Virtual MAC address is 0000.5e00.0164
```

```
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 101
  Master Router is 10.1.100.5, priority is 254
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.605 sec (expires in 2.909 sec)
```

Chapter 28 ACLs

This chapter compares the commands for configuring access control lists (ACLs).

An ACL is a list of one or more access control entries (ACEs) specifying the criteria the switch uses to either permit (forward) or deny (drop) the IP packets traversing the switch's interfaces.

This chapter covers ACL basics, creating ACLs, applying ACLs for routing/Layer 3 operations, applying ACLs for VLAN/Layer 2 operations, and applying ACLs for port/interface controls.

When using these commands, keep in mind:

- On ArubaOS-Switch and Cisco, ACLs include an Implicit Deny as the last ACE. If traffic does not match an ACL rule, it is denied (or dropped).
- On Comware, ACLs include an Implicit Allow as the last ACE. If traffic does not match an ACL rule, it is allowed.

a) Definitions of Standard or Basic ACLs and Extended or Advanced ACLs

ArubaOS-Switch

```
ArubaOS-Switch(config)# ip access-list standard ?
 NAME-STR              Specify name of Access Control List to configure.
 <1-99>                Specify Access Control List to configure by number.

ArubaOS-Switch(config)# ip access-list extended ?
 NAME-STR              Specify name of Access Control List to configure.
 <100-199>             Specify Access Control List to configure by number.
```

Comware5

```
[Comware5]acl number ?
  INTEGER<2000-2999>  Specify a basic acl
  INTEGER<3000-3999>  Specify an advanced acl
  INTEGER<4000-4999>  Specify an ethernet frame header acl

[Comware5]acl number <any-number> ?
  match-order  Set an acl's match order
  name         Specify a named acl
  <cr>

[Comware5]acl number 2000 name test2000
```

Comware7

```
[Comware7]acl number ?
  INTEGER<2000-2999>  Specify a basic ACL
  INTEGER<3000-3999>  Specify an advanced ACL
  INTEGER<4000-4999>  Specify an ethernet frame header ACL
  INTEGER<5000-5999>  Specify an ACL about user-defined frame or packet head

[Comware7]acl number 3000 ?
  match-order  Set an ACL's match order
  name         Specify a named ACL
  <cr>
```

```
[Comware7]acl number 3000 name test3000
```

Cisco

```
Cisco(config)#ip access-list standard ?
  <1-99>       Standard IP access-list number
  <1300-1999>  Standard IP access-list number (expanded range)
  WORD         Access-list name

Cisco(config)#ip access-list extended ?
  <100-199>    Extended IP access-list number
  <2000-2699>  Extended IP access-list number (expanded range)
  WORD         Access-list name
```

b) ACL Fundamental Configuration Options

Standard/Basic

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# ip access-list standard 1	[Comware]acl number 2000	Cisco(config)#ip access-list standard 1
ArubaOS-Switch(config-std-nacl)# permit 10.0.100.111 0.0.0.0	[Comware-acl-basic-2000]rule permit source 10.0.100.111 0.0.0.0	Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0
ArubaOS-Switch(config)# ip access-list standard std_acl	[Comware]acl number 2001 name std_acl	Cisco(config)#ip access-list standard std_acl
ArubaOS-Switch(config-std-nacl)# permit 10.0.100.111/32	[Comware-acl-basic-2001-std_acl]rule permit source 10.0.100.111 0	Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0

Extended/Advanced

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# ip access-list extended 100	[Comware]acl number 3000	Cisco(config)#ip access-list extended 100
ArubaOS-Switch(config-ext-nacl)# deny ip 10.1.220.0 0.0.0.255 10.0.100.111 0.0.0.0	[Comware-acl-adv-3000]rule deny ip source 10.1.220.0 0.0.0.255 destination 10.0.100. 111 0.0.0.0	Cisco(config-ext-nacl)#deny ip 10.1.220.0 0.0.0.255 10.0.100.111 0.0.0.0
ArubaOS-Switch(config-ext-nacl)# permit ip any any		Cisco(config-ext-nacl)#permit ip any any
ArubaOS-Switch(config)# ip access-list extended ext_acl	[Comware]acl number 3001 name ext_acl	Cisco(config)#ip access-list extended ext_acl
ArubaOS-Switch(config-ext-nacl)# deny ip 10.1.100.0/24 10.0.100.111/32	[Comware-acl-adv-3001-ext_acl]rule deny ip source 10.1.100.0 0.0.0.255 destination 10.0.100.111 0	Cisco(config-ext-nacl)#deny ip 10.1.100.0 0.0.0.255 10.0.100.111 0.0.0.0
ArubaOS-Switch(config-ext-nacl)# permit ip any any		Cisco(config-ext-nacl)#permit ip any any
ArubaOS-Switch(config)# access-list grouping		Cisco(config-ext-nacl)#object-group network object-group-name

ArubaOS-Switch(eth-1)# ip access-group 100 in shared		Cisco(config-ext-nacl)#host {host-address | host-name}
ArubaOS-Switch(eth-1)# ip access-group 100 out shared		Cisco(config-ext-nacl)#set security acl ip Control_Access permit host 10.1.1.10
ArubaOS-Switch(eth-1)# ipv6 access-group test in shared		Cisco(config-ext-nacl)#set security acl ip Control_Access deny 10.1.1.0 255.255.255.0
ArubaOS-Switch(eth-1)# ipv6 access-group test out shared		Cisco(config-ext-nacl)#set security acl ip CA deny tcp host 10.1.1.10 host 20.1.1.10 neq 1043
ArubaOS-Switch(eth-1)# mac-access-group 300 in shared		Cisco(config-ext-nacl)#permit tcp any any
ArubaOS-Switch(eth-1)# mac-access-group 300 out shared		
ArubaOS-Switch(vlan-1)# ip access-group 100 vlan-in shared		
ArubaOS-Switch(vlan-1)# ip access-group 100 vlan-out shared		
ArubaOS-Switch(vlan-1)# ipv6 access-group test vlan-in shared		
ArubaOS-Switch(vlan-1)# ipv6 access-group test vlan-out shared		
ArubaOS-Switch(vlan-1)# mac-access-group 300 in shared		
ArubaOS-Switch(vlan-1)# mac-access-group 300 out shared		

ArubaOS-Switch

Standard ACL

```
ArubaOS-Switch(config)# ip access-list ?
 connection-rate-fi... Configure a connection-rate-filter Access Control List.
 deny-fragmented-tc... Configure the switch to drop all IPv4 and IPv6 packets containing
                       a fragmented TCP header.
 extended              Configure an extended Access Control List.
 resequence            Renumber the entries in an Access Control List.
 standard              Configure a standard Access Control List.

ArubaOS-Switch(config)# ip access-list standard ?
 NAME-STR              Specify name of Access Control List to configure.
 <1-99>                Specify Access Control List to configure by number.

ArubaOS-Switch(config)# ip access-list standard 1
```

```
ArubaOS-Switch(config-std-nacl)# ?
 <1-2147483647>        Specify a sequence number for the ACE.
 deny                  Deny packets matching <ACL-IP-SPEC-SRC>.
 permit                Permit packets matching <ACL-IP-SPEC-SRC>.
 remark                Insert a comment into an Access Control List.

ArubaOS-Switch(config-std-nacl)# permit ?
 any                   Match packets from any IP address.
 host                  Match packets from the specified IP address.
 IP-ADDR/MASK-LENGTH   Match packets from the specified subnet.

ArubaOS-Switch(config-std-nacl)# permit 10.0.100.111 0.0.0.0


ArubaOS-Switch(config)# ip access-list standard std_acl

ArubaOS-Switch(config-std-nacl)# permit 10.0.100.111/32
```

Extended ACL

```
ArubaOS-Switch(config)# ip access-list ?
 connection-rate-fi... Configure a connection-rate-filter Access Control List.
 deny-fragmented-tc... Configure the switch to drop all IPv4 and IPv6 packets containing
                       a fragmented TCP header.
 extended              Configure an extended Access Control List.
 resequence            Renumber the entries in an Access Control List.
 standard              Configure a standard Access Control List.

ArubaOS-Switch(config)# ip access-list extended ?
 NAME-STR              Specify name of Access Control List to configure.
 <100-199>             Specify Access Control List to configure by number.

ArubaOS-Switch(config)# ip access-list extended 100

ArubaOS-Switch(config-ext-nacl)# ?
 <1-2147483647>        Specify a sequence number for the ACE.
 deny                  Deny packets matching specified parameters.
 permit                Permit packets matching specified parameters.
 remark                Insert a comment into an Access Control List.

ArubaOS-Switch(config-ext-nacl)# deny ?
<0-255>               Match a specific protocol, as further specified.
 ip-in-ip              Match IP packets, as further specified.
 ipv6-in-ip            Match IPv6 packets, as further specified.
 gre                   Match GRE packets, as further specified.
 esp                   Match ESP packets, as further specified.
 ah                    Match AH packets, as further specified.
 ospf                  Match OSPF packets, as further specified.
 pim                   Match PIM packets, as further specified.
 vrrp                  Match VRRP packets, as further specified.
 icmp                  Match ICMP packets, as further specified.
 igmp                  Match IGMP packets, as further specified.
 ip                    Match all IP packets.
 sctp                  Match SCTP packets, as further specified.
 tcp                   Match TCP packets, as further specified.
 udp                   Match UDP packets, as further specified.

ArubaOS-Switch(config-ext-nacl)# deny ip ?
 any                   Match packets from any IP address.
 host                  Match packets from the specified IP address.
```

```
 IP-ADDR/MASK-LENGTH   Match packets from the specified subnet.

ArubaOS-Switch(config-ext-nacl)# deny ip 10.0.220.0 0.0.0.255 ?
 any                   Match packets to any IP address.
 IP-ADDR/MASK-LENGTH   Match packets to the specified subnet.
 host                  Match packets to the specified IP address.

ArubaOS-Switch(config-ext-nacl)# deny ip 10.1.220.0 0.0.0.255 10.0.100.111 0.0.0.0

ArubaOS-Switch(config-ext-nacl)# permit ip any any


ArubaOS-Switch(config)# ip access-list extended ext_acl

ArubaOS-Switch(config-ext-nacl)# deny ip 10.1.100.0/24 10.0.100.111/32

ArubaOS-Switch(config-ext-nacl)# permit ip any any
```

Comware5

Basic ACL

```
[Comware5]acl ?
  copy     Specify a source acl
  ipv6     IPv6 acl
  logging  Log matched packet
  name     Specify a named acl
  number   Specify a numbered acl

[Comware5]acl number ?
  INTEGER<2000-2999>  Specify a basic acl
  INTEGER<3000-3999>  Specify an advanced acl
  INTEGER<4000-4999>  Specify an ethernet frame header acl

[Comware5]acl number 2000 ?
  match-order  Set an acl's match order
  name         Specify a named acl
  <cr>

[Comware5]acl number 2000

[Comware5-acl-basic-2000]?
Acl-basic view commands:
  cfd             Connectivity fault detection (IEEE 802.1ag)
  description     Specify ACL description
  display         Display current system information
  hardware-count  Enable hardware ACL statistics
  mtracert        Trace route to multicast source
  ping            Ping function
  quit            Exit from current command view
  return          Exit to User View
  rule            Specify an acl rule
  save            Save current configuration
  step            Specify step of acl sub rule ID
  tracert         Trace route function
  undo            Cancel current setting

[Comware5-acl-basic-2000]rule ?
  INTEGER<0-65534>  ID of acl rule
  deny              Specify matched packet deny
  permit            Specify matched packet permit
  remark            Specify Rule Remark
```

```
[Comware5-acl-basic-2000]rule permit ?
  counting      Specify Rule Counting
  fragment      Check fragment packet
  logging       Log matched packet
  source        Specify source address
  time-range    Specify a special time
  vpn-instance  Specify a VPN-Instance
  <cr>

[Comware5-acl-basic-2000]rule permit source ?
  X.X.X.X  Address of source
  any      Any source IP address

[Comware5-acl-basic-2000]rule permit source 10.0.100.111 0.0.0.0


[Comware5]acl number 2001 name std_acl

[Comware5-acl-basic-2001-std_acl]rule permit source 10.0.100.111 0
```

Advanced ACL

```
[Comware5]acl number ?
  INTEGER<2000-2999>  Specify a basic acl
  INTEGER<3000-3999>  Specify an advanced acl
  INTEGER<4000-4999>  Specify an ethernet frame header acl

[Comware5]acl number 3000 ?
  match-order  Set an acl's match order
  name         Specify a named acl
  <cr>

[Comware5]acl number 3000

[Comware5-acl-adv-3000]?
Acl-adv view commands:
  cfd             Connectivity fault detection (IEEE 802.1ag)
  description     Specify ACL description
  display         Display current system information
  hardware-count  Enable hardware ACL statistics
  mtracert        Trace route to multicast source
  ping            Ping function
  quit            Exit from current command view
  return          Exit to User View
  rule            Specify an acl rule
  save            Save current configuration
  step            Specify step of acl sub rule ID
  tracert         Trace route function
  undo            Cancel current setting

[Comware5-acl-adv-3000]rule ?
  INTEGER<0-65534>  ID of acl rule
  deny              Specify matched packet deny
  permit            Specify matched packet permit
  remark            Specify Rule Remark

[Comware5-acl-adv-3000]rule deny ?
  <0-255>  Protocol number
  gre      GRE tunneling(47)
  icmp     Internet Control Message Protocol(1)
```

```
  igmp     Internet Group Management Protocol(2)
  ip       Any IP protocol
  ipinip   IP in IP tunneling(4)
  ospf     OSPF routing protocol(89)
  tcp      Transmission Control Protocol (6)
  udp      User Datagram Protocol (17)

[Comware5-acl-adv-3000]rule deny ip ?
  counting      Specify Rule Counting
  destination   Specify destination address
  dscp          Differentiated Services Codepoint (DSCP)
  fragment      Check fragment packet
  logging       Log matched packet
  precedence    Specify precedence
  source        Specify source address
  time-range    Specify a special time
  tos           Specify tos
  vpn-instance  Specify a VPN-Instance
  <cr>

[Comware5-acl-adv-3000]rule deny ip source ?
  X.X.X.X  Address of source
  any      Any source IP address

[Comware5-acl-adv-3000]rule deny ip source 10.1.220.0 0.0.0.255 ?
  counting      Specify Rule Counting
  destination   Specify destination address
  dscp          Differentiated Services Codepoint (DSCP)
  fragment      Check fragment packet
  logging       Log matched packet
  precedence    Specify precedence
  time-range    Specify a special time
  tos           Specify tos
  vpn-instance  Specify a VPN-Instance
  <cr>

[Comware5-acl-adv-3000]rule deny ip source 10.1.220.0 0.0.0.255 destination ?
  X.X.X.X  Address of destination
  any      Any destination IP address

[Comware5-acl-adv-3000]rule deny ip source 10.1.220.0 0.0.0.255 destination 10.0.100.
111 0.0.0.0


[Comware5]acl number 3001 name ext_acl

[Comware5-acl-adv-3001-ext_acl]rule deny ip source 10.1.100.0 0.0.0.255 destination
10.0.100.111 0
```

Comware7

Basic ACL

```
[Comware7]acl ?
  copy     Specify a source ACL
  ipv6     IPv6 ACL
  logging  Log matched packet
  name     Specify a named ACL
  number   Specify a numbered ACL

[Comware7]acl number ?
  INTEGER<2000-2999>  Specify a basic ACL
```

```
  INTEGER<3000-3999>  Specify an advanced ACL
  INTEGER<4000-4999>  Specify an ethernet frame header ACL
  INTEGER<5000-5999>  Specify an ACL about user-defined frame or packet head

[Comware7]acl number 2000 ?
  match-order  Set an ACL's match order
  name         Specify a named ACL
  <cr>

[Comware7]acl number 2000

[Comware7-acl-basic-2000]?
Acl-basic view commands:
  cfd                 Connectivity Fault Detection (CFD) module
  description         Specify ACL description
  diagnostic-logfile  Diagnostic log file configuration
  display             Display current system information
  logfile             Log file configuration
  monitor             System monitor
  ping                Ping function
  quit                Exit from current command view
  return              Exit to User View
  rule                Specify an ACL rule
  save                Save current configuration
  security-logfile    Security log file configuration
  step                Specify a rule numbering step for an ACL
  tracert             Tracert function
  undo                Cancel current setting

[Comware7-acl-basic-2000]rule ?
  INTEGER<0-65534>  ID of an ACL rule
  deny              Specify matched packet deny
  permit            Specify matched packet permit

[Comware7-acl-basic-2000]rule permit ?
  counting      Specify rule counting
  fragment      Check fragment packet
  logging       Log matched packet
  source        Specify a source address
  time-range    Specify a special time
  vpn-instance  Specify VPN-Instance
  <cr>

[Comware7-acl-basic-2000]rule permit source ?
  X.X.X.X  Address of source
  any      Any source IP address

[Comware7-acl-basic-2000]rule permit source 10.0.100.111 0.0.0.0


[Comware7]acl number 2001 name std_acl

[Comware7-acl-basic-2001-std_acl]rule permit source 10.0.100.111 0
```

Advanced ACL

```
[Comware7]acl number ?
  INTEGER<2000-2999>  Specify a basic ACL
  INTEGER<3000-3999>  Specify an advanced ACL
  INTEGER<4000-4999>  Specify an ethernet frame header ACL
  INTEGER<5000-5999>  Specify an ACL about user-defined frame or packet head
```

```
[Comware7]acl number 3000 ?
  match-order  Set an ACL's match order
  name         Specify a named ACL
  <cr>

[Comware7]acl number 3000

[Comware7-acl-adv-3000]?
Acl-adv view commands:
  cfd                 Connectivity Fault Detection (CFD) module
  description         Specify ACL description
  diagnostic-logfile  Diagnostic log file configuration
  display             Display current system information
  logfile             Log file configuration
  monitor             System monitor
  ping                Ping function
  quit                Exit from current command view
  return              Exit to User View
  rule                Specify an ACL rule
  save                Save current configuration
  security-logfile    Security log file configuration
  step                Specify a rule numbering step for an ACL
  tracert             Tracert function
  undo                Cancel current setting

[Comware7-acl-adv-3000]rule ?
  INTEGER<0-65534>  ID of an ACL rule
  deny              Specify matched packet deny
  permit            Specify matched packet permit

[Comware7-acl-adv-3000]rule deny ?
  INTEGER<0-255>  Protocol number
  gre             GRE tunneling (47)
  icmp            Internet Control Message Protocol (1)
  igmp            Internet Group Management Protocol (2)
  ip              Any IP protocol
  ipinip          IP in IP tunneling (4)
  ospf            OSPF routing protocol (89)
  tcp             Transmission Control Protocol (6)
  udp             User Datagram Protocol (17)

[Comware7-acl-adv-3000]rule deny ip ?
  counting      Specify rule counting
  destination   Specify a destination address
  dscp          Specify DSCP
  fragment      Check fragment packet
  logging       Log matched packet
  precedence    Specify precedence
  source        Specify a source address
  time-range    Specify a special time
  tos           Specify TOS
  vpn-instance  Specify VPN-Instance
  <cr>

[Comware7-acl-adv-3000]rule deny ip source ?
  X.X.X.X  Source address
  any      Any source address

[Comware7-acl-adv-3000]rule deny ip source 10.1.220.0 0.0.0.255 ?
  counting      Specify rule counting
  destination   Specify a destination address
  dscp          Specify DSCP
```

```
  fragment      Check fragment packet
  logging       Log matched packet
  precedence    Specify precedence
  time-range    Specify a special time
  tos           Specify TOS
  vpn-instance  Specify VPN-Instance
  <cr>

[Comware7-acl-adv-3000]rule deny ip source 10.1.220.0 0.0.0.255 destination ?
  X.X.X.X  Destination address
  any      Any destination address

[Comware7-acl-adv-3000]rule deny ip source 10.1.220.0 0.0.0.255 destination 10.0.100.
111 0.0.0.0


[Comware7]acl number 3001 name ext_acl

[Comware7-acl-adv-3001-ext_acl]rule deny ip source 10.1.100.0 0.0.0.255 destination
10.0.100.111 0
```

Cisco

Standard ACL

```
Cisco(config)#ip access-list ?
  extended    Extended Access List
  log-update  Control access list log updates
  logging     Control access list logging
  resequence  Resequence Access List
  role-based  Role-based Access List
  standard    Standard Access List

Cisco(config)#ip access-list standard ?
  <1-99>       Standard IP access-list number
  <1300-1999>  Standard IP access-list number (expanded range)
  WORD         Access-list name

Cisco(config)#ip access-list standard 1

Cisco(config-std-nacl)#?
Standard Access List configuration commands:
  <1-2147483647>  Sequence Number
  default         Set a command to its defaults
  deny            Specify packets to reject
  exit            Exit from access-list configuration mode
  no              Negate a command or set its defaults
  permit          Specify packets to forward
  remark          Access list entry comment

Cisco(config-std-nacl)#permit ?
  Hostname or A.B.C.D  Address to match
  any                  Any source host
  host                 A single host address

Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0


Cisco(config)#ip access-list standard std_acl

Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0
```

Extended ACL

```
Cisco(config)#ip access-list ?
  extended    Extended Access List
  log-update  Control access list log updates
  logging     Control access list logging
  resequence  Resequence Access List
  role-based  Role-based Access List
  standard    Standard Access List

Cisco(config)#ip access-list extended ?
  <100-199>    Extended IP access-list number
  <2000-2699>  Extended IP access-list number (expanded range)
  WORD         Access-list name

Cisco(config)#ip access-list extended 100

Cisco(config-ext-nacl)#?
Ext Access List configuration commands:
  <1-2147483647>  Sequence Number
  default         Set a command to its defaults
  deny            Specify packets to reject
  dynamic         Specify a DYNAMIC list of PERMITs or DENYs
  evaluate        Evaluate an access list
  exit            Exit from access-list configuration mode
  no              Negate a command or set its defaults
  permit          Specify packets to forward
  remark          Access list entry comment

Cisco(config-ext-nacl)#deny ?
  <0-255>  An IP protocol number
  ahp      Authentication Header Protocol
  eigrp    Cisco's EIGRP routing protocol
  esp      Encapsulation Security Payload
  gre      Cisco's GRE tunneling
  icmp     Internet Control Message Protocol
  igmp     Internet Gateway Message Protocol
  ip       Any Internet Protocol
  ipinip   IP in IP tunneling
  nos      KA9Q NOS compatible IP over IP tunneling
  ospf     OSPF routing protocol
  pcp      Payload Compression Protocol
  pim      Protocol Independent Multicast
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol

Cisco(config-ext-nacl)#deny ip ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host

Cisco(config-ext-nacl)#deny ip 10.1.220.0 0.0.0.255 ?
  A.B.C.D  Destination address
  any      Any destination host
  host     A single destination host

Cisco(config-ext-nacl)#deny ip 10.1.220.0 0.0.0.255 10.0.100.111 0.0.0.0

Cisco(config-ext-nacl)#permit ip any any

Cisco(config)#ip access-list extended ext_acl
```

```
Cisco(config-ext-nacl)#deny ip 10.1.100.0 0.0.0.255 10.0.100.111 0.0.0.0

Cisco(config-ext-nacl)#permit ip any any
```

c) Routed/Layer 3 ACL (RACL)

On ArubaOS-Switch, you configure a RACL on a VLAN to filter:

- Routed traffic arriving on or sent from the switch on the VLAN
- Traffic with a destination on the switch itself

On Comware , you can apply an ACL to filter packets to a Layer 3 interface to regulate traffic in a specific direction (inbound or outbound).

On Cisco, RACLs access-control routed traffic between VLANs and are applied to Layer 3 interfaces in a specific direction (inbound or outbound).

Standard or Basic ACL

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# ip access-list standard 1	[Comware]acl number 2000	Cisco(config)#ip access-list standard 1
ArubaOS-Switch(config-std-nacl)# permit 10.0.100.111 0.0.0.0	[Comware-acl-basic-2000]rule permit source 10.0.100.111 0.0.0.0	Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0
ArubaOS-Switch(config)# ip access-list standard std_acl	[Comware]acl number 2001 name std_acl	Cisco(config)#ip access-list standard std_acl
ArubaOS-Switch(config-std-nacl)# permit 10.0.100.111/32	[Comware-acl-basic-2001-std_acl]rule permit source 10.0.100.111 0	Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0
ArubaOS-Switch(config-std-nacl)# vlan 220	[Comware-acl-basic-2001-std_acl]quit [Comware]interface Vlan-interface 220	Cisco(config-std-nacl)#interface vlan 220
ArubaOS-Switch(vlan-220)# ip access-group 1 in	[Comware-Vlan-interface220]packet-filter 2000 inbound	Cisco(config-if)#ip access-group 1 in
ArubaOS-Switch(config)# vlan 100	[Comware]interface Vlan-interface 100	Cisco(config)#interface vlan 100
ArubaOS-Switch(vlan-100)# ip access-group std_acl in	[Comware-Vlan-interface100]packet-filter 2001 inbound	Cisco(config-if)#ip access-group std_acl in

Extended or Advanced ACL

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# ip access-list extended 100	[Comware]acl number 3000	Cisco(config)#ip access-list extended 100
ArubaOS-Switch(config-ext-nacl)# deny ip 10.1.220.0 0.0.0.255 10.0.100.111 0.0.0.0	[Comware-acl-adv-3000]rule deny ip source 10.1.220.0 0.0.0.255 destination 10.1.100.111 0	Cisco(config-ext-nacl)#deny ip 10.1.220.0 0.0.0.255 10.0.100.111 0.0.0.0

ArubaOS-Switch(config-ext-nacl)# permit ip any any		Cisco(config-ext-nacl)#permit ip any any
ArubaOS-Switch(config)# ip access-list extended ext_acl	[Comware]acl number 3001 name ext_acl	Cisco(config)#ip access-list extended ext_acl
ArubaOS-Switch(config-ext-nacl)# deny ip 10.1.100.0/24 10.0.100.111/32	[Comware-acl-adv-3001-ext_acl]rule deny ip source 10.1.100.0 0.0.0.255 destination 10.0.100.111 0	Cisco(config-ext-nacl)#deny ip 10.1.100.0 255.255.255.0 10.0.100.111 255.255.255.255
ArubaOS-Switch(config-ext-nacl)# permit ip any any		Cisco(config-ext-nacl)#permit ip any any
ArubaOS-Switch(config)# vlan 220	[Comware-acl-adv-3001-ext_acl]quit [Comware]interface Vlan-interface 220	Cisco(config)#interface vlan 220
ArubaOS-Switch(vlan-220)# ip access-group 100 in	[Comware-Vlan-interface220]packet-filter 3000 inbound	Cisco(config-if)#ip access-group 100 in
ArubaOS-Switch(vlan-220)# vlan 100	[Comware]interface Vlan-interface 100	Cisco(config-if)#interface vlan 100
ArubaOS-Switch(vlan-100)# ip access-group ext_acl in	[Comware-Vlan-interface100]packet-filter 3001 inbound	Cisco(config-if)#ip access-group ext_acl in

ArubaOS-Switch

Standard ACL

```
ArubaOS-Switch(config)# ip access-list standard 1

ArubaOS-Switch(config-std-nacl)# permit 10.0.100.111 0.0.0.0


ArubaOS-Switch(config)# ip access-list standard std_acl

ArubaOS-Switch(config-std-nacl)# permit 10.0.100.111/32


ArubaOS-Switch(config-std-nacl)# vlan 220

ArubaOS-Switch(vlan-220)# ip access-group ?
 ASCII-STR             Enter an ASCII string for the 'access-group'
                       command/parameter.

ArubaOS-Switch(vlan-220)# ip access-group 1 ?
 in                    Match inbound packets
 out                   Match outbound packets
 connection-rate-filter Manage packet rates
 vlan                  VLAN acl

ArubaOS-Switch(vlan-220)# ip access-group 1 in


ArubaOS-Switch(config)# vlan 100

ArubaOS-Switch(vlan-100)# ip access-group std_acl in
```

Extended ACL

```
ArubaOS-Switch(config)# ip access-list extended 100

ArubaOS-Switch(config-ext-nacl)# deny ip 10.1.220.0 0.0.0.255 10.0.100.111 0.0.0.0

ArubaOS-Switch(config-ext-nacl)# permit ip any any


ArubaOS-Switch(config)# ip access-list extended ext_acl

ArubaOS-Switch(config-ext-nacl)# deny ip 10.1.100.0/24 10.0.100.111/32

ArubaOS-Switch(config-ext-nacl)# permit ip any any


ArubaOS-Switch(config)# vlan 220

ArubaOS-Switch(vlan-220)# ip access-group 100 in


ArubaOS-Switch(vlan-220)# vlan 100

ArubaOS-Switch(vlan-100)# ip access-group ext_acl in
```

Comware5

Basic ACL

```
[Comware5]acl number 2000

[Comware5-acl-basic-2000]rule permit source 10.0.100.111 0.0.0.0


[Comware5]acl number 2001 name ext_acl

[Comware5-acl-basic-2001-ext_acl]rule permit source 10.0.100.111 0


[Comware5]interface Vlan-interface 220

[Comware5-Vlan-interface220]packet-filter ?
  INTEGER<2000-2999>  Apply basic acl
  INTEGER<3000-3999>  Apply advanced acl
  INTEGER<4000-4999>  Apply ethernet frame header acl
  ipv6                IPv6 ACL
  name                Specify a named acl

[Comware5-Vlan-interface220]packet-filter 2000 ?
  inbound   Apply the acl to filter in-bound packets
  outbound  Apply the acl to filter out-bound packets

[Comware5-Vlan-interface220]packet-filter 2000 inbound ?
  <cr>

[Comware5-Vlan-interface220]packet-filter 2000 inbound


[Comware5]interface Vlan-interface 100

[Comware5-Vlan-interface100]packet-filter 2001 inbound
```

Advanced ACL

```
[Comware5]acl number 3000

[Comware5-acl-adv-3000]rule deny ip source 10.1.220.0 0.0.0.255 destination 10.1.100.111 0


[Comware5]acl number 3001 name ext_acl

[Comware5-acl-adv-3001-ext_acl]rule deny ip source 10.1.100.0 0.0.0.255 destination
10.0.100.111 0


[Comware5-acl-adv-3001-ext_acl]quit

[Comware]interface Vlan-interface 220

[Comware5-Vlan-interface220]packet-filter 3000 inbound


[Comware5]interface Vlan-interface 100

[Comware5-Vlan-interface100]packet-filter 3001 inbound
```

Comware7

Basic ACL

```
[Comware7]acl number 2000

[Comware7-acl-basic-2000]rule permit source 10.0.100.111 0.0.0.0


[Comware7]acl number 2001 name ext_acl

[Comware7-acl-basic-2001-ext_acl]rule permit source 10.0.100.111 0


[Comware7]interface Vlan-interface 220

[Comware7-Vlan-interface220]packet-filter ?
  INTEGER<2000-2999>  Specify a basic ACL
  INTEGER<3000-3999>  Specify an advanced ACL
  INTEGER<4000-4999>  Specify an ethernet frame header ACL
  INTEGER<5000-5999>  Specify an ACL about user-defined frame or packet head
  filter              Specify the packet filter mode
  ipv6                IPv6 ACL
  name                Specify a named ACL

[Comware7-Vlan-interface220]packet-filter 2000 ?
  inbound   Filter incoming packets
  outbound  Filter outgoing packets

[Comware7-Vlan-interface220]packet-filter 2000 inbound ?
  hardware-count  Count rule matches performed by hardware
  <cr>

[Comware7-Vlan-interface220]packet-filter 2000 inbound


[Comware7]interface Vlan-interface 100
```

```
[Comware7-Vlan-interface100]packet-filter 2001 inbound
```

Advanced ACL

```
[Comware7]acl number 3000

[Comware7-acl-adv-3000]rule deny ip source 10.1.220.0 0.0.0.255 destination 10.1.100.111 0


[Comware7]acl number 3001 name ext_acl

[Comware7-acl-adv-3001-ext_acl]rule deny ip source 10.1.100.0 0.0.0.255 destination
10.0.100.111 0


[Comware7-acl-adv-3001-ext_acl]quit

[Comware7]interface Vlan-interface 220

[Comware7-Vlan-interface220]packet-filter 3000 inbound


[Comware7]interface Vlan-interface 100

[Comware7-Vlan-interface100]packet-filter 3001 inbound
```

Cisco

Standard ACL

```
Cisco(config)#ip access-list standard 1

Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0


Cisco(config)#ip access-list standard std_acl

Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0


Cisco(config)#interface vlan 220

Cisco(config-if)#ip access-group ?
  <1-199>      IP access list (standard or extended)
  <1300-2699>  IP expanded access list (standard or extended)
  WORD         Access-list name

Cisco(config-if)#ip access-group 1 ?
  in   inbound packets
  out  outbound packets

Cisco(config-if)#ip access-group 1 in


Cisco(config)#interface vl 100

Cisco(config-if)#ip access-group std_acl in
```

Extended ACL

```
Cisco(config)#ip access-list extended 100
Cisco(config-ext-nacl)#deny ip 10.1.220.0 0.0.0.255 10.0.100.111 0.0.0.0
Cisco(config-ext-nacl)#permit ip any any

Cisco(config)#ip access-list extended ext_acl
Cisco(config-ext-nacl)#deny ip 10.1.100.0 255.255.255.0 10.0.100.111 255.255.255.255
Cisco(config-ext-nacl)#permit ip any any

Cisco(config-ext-nacl)#interface vlan 220
Cisco(config-if)#ip access-group 100 in

Cisco(config-if)#interface vlan 100
Cisco(config-if)#ip access-group ext_acl in
```

d) VLAN/Layer 2 Based ACL (VACL)

On ArubaOS-Switch, a VLAN ACL is an ACL that you configure on a VLAN to filter traffic entering the switch on that VLAN interface and having a destination on the same VLAN.

On Comware, you can apply Ethernet frame header ACLs, also called "Layer 2 ACLs," to match packets based on Layer 2 protocol header fields such as source MAC address, destination MAC address, 802.1p priority (VLAN priority), or link layer protocol type.

On Cisco, VLAN ACLs or VLAN maps are used to access-control all packets, whether they are bridged or routed. VLAN maps can also filter traffic between devices in the same VLAN. You configure VLAN maps to provide access control based on Layer 3 addresses. Unsupported protocols are access-controlled through MAC addresses using Ethernet ACEs. After a VLAN map is applied to a VLAN, all packets (either routed or bridged) entering the VLAN are checked against the VLAN map.

Standard or Basic ACL

ArubaOS-Switch	Comware	Cisco
`ArubaOS-Switch(config)# ip access-list standard 10`	`[Comware]acl number 4000`	Step - 1
`ArubaOS-Switch(config-std-nacl)# deny 10.1.220.102 0.0.0.0`	`[Comware-acl-ethernetframe-4000]rule deny dest-mac 00aa-bb00-0000 00aa-bbff-ffff`	`Cisco(config)#access-list 10 permit host 10.1.220.102`
`ArubaOS-Switch(config)# ip access-list standard std_vacl`		Step - 2
`ArubaOS-Switch(config-std-nacl)# deny 10.1.220.103/32`		`Cisco(config)#vlan access-map vacl_1 10`
`ArubaOS-Switch(config-std-nacl)# vlan 220`	`[Comware]interface Vlan-interface 220`	`Cisco(config-access-map)#match ip address 10`
`ArubaOS-Switch(vlan-220)# ip access-group 10 vlan`	`[Comware-Vlan-interface220]packet-filter 4000 in`	`Cisco(config-access-map)#action drop`
		Step - 3
		`Cisco(config)#vlan filter vacl_1 vlan-list 220`

Extended or Advanced ACL

ArubaOS-Switch	Comware	Cisco
`ArubaOS-Switch(config)# ip access-list extended 110`	Note: only one ACL number for this type of ACL available.	Step - 1
`ArubaOS-Switch(config-ext-nacl)# deny ip 10.1.220.0 0.0.0.255 10. 1.220.102 0.0.0.0`		`Cisco(config)#access-list 110 permit icmp any host 10.1.220.102`
`ArubaOS-Switch(config-ext-nacl)# permit ip any any`		`Cisco(config)#access-list 111 permit icmp any any`
`ArubaOS-Switch(config)# ip access-list extended ext_vacl`		Step - 2
`ArubaOS-Switch(config-ext-nacl)# deny ip 10.1.220.0/24 10.1.220.103/32`		`Cisco(config)#vlan access-map vacl_2 10`

ArubaOS-Switch(config-ext-nacl)# permit ip any any		Cisco(config-access-map)#match ip address 110
ArubaOS-Switch(config)# vlan 220		Cisco(config-access-map)#action drop
ArubaOS-Switch(vlan-220)# ip access-group 110 vlan		Cisco(config)#vlan access-map vacl_2 20
		Cisco(config-access-map)#match ip address 111
		Cisco(config-access-map)#action forward
		Step - 3
		Cisco(config)#vlan filter vacl_2 vlan-list 220

ArubaOS-Switch

Standard ACL

```
ArubaOS-Switch(config)# ip access-list standard 10

ArubaOS-Switch(config-std-nacl)# deny 10.1.220.102 0.0.0.0


ArubaOS-Switch(config)# ip access-list standard std_vacl

ArubaOS-Switch(config-std-nacl)# deny 10.1.220.103/32


ArubaOS-Switch(config)# vlan 220

ArubaOS-Switch(vlan-220)# ip access-group 1 ?
 in                     Match inbound packets
 out                    Match outbound packets
 connection-rate-filter Manage packet rates
 vlan                   VLAN acl

ArubaOS-Switch(vlan-220)# ip access-group 10 vlan

ArubaOS-Switch(vlan-220)# ip access-group std_vacl vlan
```

Extended ACL

```
ArubaOS-Switch(config)# ip access-list extended 110

ArubaOS-Switch(config-ext-nacl)# deny ip 10.1.220.0 0.0.0.255 10.1.220.102 0.0.0.0

ArubaOS-Switch(config-ext-nacl)# permit ip any any


ArubaOS-Switch(config)# ip access-list extended ext_vacl

ArubaOS-Switch(config-ext-nacl)# deny ip 10.1.220.0/24 10.1.220.103/32

ArubaOS-Switch(config-ext-nacl)# permit ip any any


ArubaOS-Switch(config)# vlan 220
```

```
ArubaOS-Switch(vlan-220)# ip access-group 110 ?
 in                     Match inbound packets
 out                    Match outbound packets ?
 connection-rate-filter Manage packet rates
 vlan                   VLAN acl

ArubaOS-Switch(vlan-220)# ip access-group 110 vlan

ArubaOS-Switch(vlan-220)# ip access-group ext_vacl vlan
```

Comware5

Ethernet frame header ACL

```
[Comware5]acl number ?
  INTEGER<2000-2999>  Specify a basic acl
  INTEGER<3000-3999>  Specify an advanced acl
  INTEGER<4000-4999>  Specify an ethernet frame header acl

[Comware5]acl number 4000

[Comware5-acl-ethernetframe-4000]?
Acl-ethernetframe view commands:
  cfd             Connectivity fault detection (IEEE 802.1ag)
  description     Specify ACL description
  display         Display current system information
  hardware-count  Enable hardware ACL statistics
  mtracert        Trace route to multicast source
  ping            Ping function
  quit            Exit from current command view
  return          Exit to User View
  rule            Specify an acl rule
  save            Save current configuration
  step            Specify step of acl sub rule ID
  tracert         Trace route function
  undo            Cancel current setting

[Comware5-acl-ethernetframe-4000]rule ?
  INTEGER<0-65534>  ID of acl rule
  deny              Specify matched packet deny
  permit            Specify matched packet permit
  remark            Specify Rule Remark

[Comware5-acl-ethernetframe-4000]rule deny ?
  cos         Specify 802.1p priority
  counting    Specify Rule Counting
  dest-mac    Specify dest mac address
  lsap        Specify lsap type
  source-mac  Specify source mac address
  time-range  Specify a special time
  type        Specify protocol type
  <cr>

[Comware5-acl-ethernetframe-4000]rule deny dest-mac ?
  H-H-H  48-bit hardware address
```

```
[Comware5-acl-ethernetframe-4000]rule deny dest-mac 00aa-bbcc-ddee ?
  H-H-H  48-bit hardware address mask

[Comware5-acl-ethernetframe-4000]rule deny source-mac 00aa-bb00-0000 0000-00ff-ffff ?
  cos         Specify 802.1p priority
  counting    Specify Rule Counting
  lsap        Specify lsap type
  source-mac  Specify source mac address
  time-range  Specify a special time
  type        Specify protocol type
  <cr>

[Comware5-acl-ethernetframe-4000]rule deny dest-mac 00aa-bb00-0000 00aa-bbff-ffff


[Comware5]interface Vlan-interface 220

[Comware5-Vlan-interface220]packet-filter 4000 out
```

Comware7

Ethernet frame header ACL

```
[Comware7]acl number ?
  INTEGER<2000-2999>  Specify a basic ACL
  INTEGER<3000-3999>  Specify an advanced ACL
  INTEGER<4000-4999>  Specify an ethernet frame header ACL
  INTEGER<5000-5999>  Specify an ACL about user-defined frame or packet head

[Comware7]acl number 4000

[Comware7-acl-ethernetframe-4000]?
Acl-ethernetframe view commands:
  cfd                 Connectivity Fault Detection (CFD) module
  description         Specify ACL description
  diagnostic-logfile  Diagnostic log file configuration
  display             Display current system information
  logfile             Log file configuration
  monitor             System monitor
  ping                Ping function
  quit                Exit from current command view
  return              Exit to User View
  rule                Specify an ACL rule
  save                Save current configuration
  security-logfile    Security log file configuration
  step                Specify a rule numbering step for an ACL
  tracert             Tracert function
  undo                Cancel current setting

[Comware7-acl-ethernetframe-4000]rule ?
  INTEGER<0-65534>  ID of an ACL rule
  deny              Specify matched packet deny
  permit            Specify matched packet permit
```

```
[Comware7-acl-ethernetframe-4000]rule deny ?
  cos         Specify 802.1p priority
  counting    Specify rule counting
  dest-mac    Specify dest mac address
  lsap        Specify lsap type
  source-mac  Specify source mac address
  time-range  Specify a special time
  type        Specify protocol type
  <cr>

[Comware7-acl-ethernetframe-4000]rule deny dest-mac ?
  H-H-H  48-bit hardware address

[Comware7-acl-ethernetframe-4000]rule deny dest-mac 00aa-bbcc-ddee ?
  H-H-H  48-bit hardware address mask

[Comware7-acl-ethernetframe-4000]rule deny source-mac 00aa-bb00-0000 0000-00ff-ffff ?
  cos         Specify 802.1p priority
  counting    Specify rule counting
  lsap        Specify lsap type
  source-mac  Specify source mac address
  time-range  Specify a special time
  type        Specify protocol type
  <cr>

[Comware7-acl-ethernetframe-4000]rule deny dest-mac 00aa-bb00-0000 00aa-bbff-ffff


[Comware7]interface Vlan-interface 220

[Comware7-Vlan-interface220]packet-filter 4000 out
```

Cisco

Standard ACL

step-1

```
Cisco(config)#access-list 10 permit host 10.1.220.102
```

step-2

```
Cisco(config)#vlan ?
  WORD           ISL VLAN IDs 1-4094
  access-log     Configure VACL logging
  access-map     Create vlan access-map or enter vlan access-map command mode
  configuration  vlan feature configuration mode
  dot1q          dot1q parameters
  filter         Apply a VLAN Map
  group          Create a vlan group
  internal       internal VLAN

Cisco(config)#vlan access-map ?
  WORD  Vlan access map tag

Cisco(config)#vlan access-map vacl_1 ?
```

```
  <0-65535>  Sequence to insert to/delete from existing vlan access-map entry
  <cr>

Cisco(config)#vlan access-map vacl_1 10

Cisco(config-access-map)#?
Vlan access-map configuration commands:
  action   Take the action
  default  Set a command to its defaults
  exit     Exit from vlan access-map configuration mode
  match    Match values.
  no       Negate a command or set its defaults


Cisco(config-access-map)#match ?
  ip   IP based match
  mac  MAC based match

Cisco(config-access-map)#match ip ?
  address  Match IP address to access control.

Cisco(config-access-map)#match ip address ?
  <1-199>      IP access list (standard or extended)
  <1300-2699>  IP expanded access list (standard or extended)
  WORD         Access-list name

Cisco(config-access-map)#match ip address 10 ?
  <1-199>      IP access list (standard or extended)
  <1300-2699>  IP expanded access list (standard or extended)
  WORD         Access-list name
  <cr>

Cisco(config-access-map)#match ip address 10

Cisco(config-access-map)#action ?
  drop     Drop packets
  forward  Forward packets

Cisco(config-access-map)#action drop ?
  log  Log dropped packets
  <cr>

Cisco(config-access-map)#action drop
```

step-3

```
Cisco(config)#vlan filter ?
  WORD  VLAN map name

Cisco(config)#vlan filter vacl_1 ?
  vlan-list  VLANs to apply filter to

Cisco(config)#vlan filter vacl_1 vlan-list ?
  <1-4094>  VLAN id
  all       Add this filter to all VLANs

Cisco(config)#vlan filter vacl_1 vlan-list 220 ?
  ,  comma
  -  hyphen
  <cr>

Cisco(config)#vlan filter vacl_1 vlan-list 220
```

Extended ACL

step-1

```
Cisco(config)#access-list 110 permit icmp any host 10.1.220.102

Cisco(config)#access-list 111 permit icmp any any
```

step-2

```
Cisco(config)#vlan access-map ?
  WORD  Vlan access map tag

Cisco(config)#vlan access-map vacl_2 ?
  <0-65535>  Sequence to insert to/delete from existing vlan access-map entry
  <cr>

Cisco(config)#vlan access-map vacl_2 10 ?
  <cr>

Cisco(config)#vlan access-map vacl_2 10


Cisco(config-access-map)#?
Vlan access-map configuration commands:
  action   Take the action
  default  Set a command to its defaults
  exit     Exit from vlan access-map configuration mode
  match    Match values.
  no       Negate a command or set its defaults

Cisco(config-access-map)#match ip address ?
  <1-199>      IP access list (standard or extended)
  <1300-2699>  IP expanded access list (standard or extended)
  WORD         Access-list name

Cisco(config-access-map)#match ip address 110


Cisco(config-access-map)#action ?
  drop     Drop packets
  forward  Forward packets

Cisco(config-access-map)#action drop ?
  <cr>

Cisco(config-access-map)#action drop

Cisco(config-access-map)#exit

Cisco(config)#vlan access-map vacl_2 20

Cisco(config-access-map)#match ip address 111

Cisco(config-access-map)#action forward
```

step-3

```
Cisco(config)#vlan filter vacl_2 vlan-list 220
```

e) Port ACL (PACL)

On ArubaOS-Switch, you configure a Static Port ACL on a port to filter traffic entering the switch on that port, regardless of whether the traffic is routed, switched, or addressed to a destination on the switch itself.

On Comware, you can apply a single packet filter to an interface in a specific direction (inbound or outbound).

On Cisco, a Port ACL access-controls traffic entering a Layer 2 interface.

Standard or Basic ACL

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# ip access-list standard 11	[Comware]acl number 2011	Cisco(config)#ip access-list standard 11
ArubaOS-Switch(config-std-nacl)# permit 10.0.100.111 0.0.0.0	[Comware-acl-basic-2011]rule permit source 10.0.100.111 0	Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0
ArubaOS-Switch(config)# ip access-list standard std_pacl	[Comware]acl number 2012 name std_pacl	Cisco(config)#ip access-list standard std_pacl
ArubaOS-Switch(config-std-nacl)# permit 10.0.100.111/32	[Comware-acl-basic-2012-std_pacl]rule permit source 10.0.100.111 0	Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0
ArubaOS-Switch(config)# interface 4	[Comware]interface g1/0/4	Cisco(config)#interface g1/0/4
ArubaOS-Switch(eth-4)# ip access-group 11 in	[Comware-GigabitEthernet1/0/4] packet-filter 2011 inbound	Cisco(config-if)#ip access-group 11 in
ArubaOS-Switch(eth-4)# ip access-group std_pacl in	[Comware-GigabitEthernet1/0/4] packet-filter 2012 inbound	Cisco(config-if)#ip access-group std_pacl in

Extended or Advanced ACL

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# ip access-list extended 111	[Comware]acl number 3011	Cisco(config)#ip access-list extended 121
ArubaOS-Switch(config-ext-nacl)# deny ip 10.1.220.0 0.0.0.255 10.0.100.111 0.0.0.0	[Comware-acl-adv-3011]rule deny ip source 10.1.220.0 0.0.0.255 destination 10.0.100.111 0	Cisco(config-ext-nacl)#deny ip 10.1.220.0 0.0.0.255 10.0.100.111 0.0.0.0
ArubaOS-Switch(config-ext-nacl)# permit ip any any		Cisco(config-ext-nacl)#permit ip any any
ArubaOS-Switch(config)# ip access-list extended ext_pacl	[Comware]acl number 3012 name ext_pacl	Cisco(config)#ip access-list extended ext_pacl
ArubaOS-Switch(config-ext-nacl)# deny ip 10.1.220.0/24 10.0.100.111/32	[Comware-acl-adv-3012-ext_acl]rule deny ip source 10.1.220.0 0.0.0.255 destination	Cisco(config-ext-nacl)#deny ip 10.1.220.0 255.255.255.0 10.0.100.111 255.255.255.255

	10.0.100.111 0	
ArubaOS-Switch(config-ext-nacl)# permit ip any any		Cisco(config-ext-nacl)#permit ip any any
ArubaOS-Switch(config)# interface 4	[Comware]interface g1/0/4	Cisco(config)#interface g1/0/4
ArubaOS-Switch(eth-4)# ip access-group 111 in	[Comware-GigabitEthernet1/0/4] packet-filter 3011 inbound	Cisco(config-if)#ip access-group 121 in
ArubaOS-Switch(eth-4)# ip access-group ext_pacl in	[Comware-GigabitEthernet1/0/4] packet-filter 3012 inbound	Cisco(config-if)#ip access-group ext_pacl in

ArubaOS-Switch

Standard ACL

```
ArubaOS-Switch(config)# ip access-list standard 11

ArubaOS-Switch(config-std-nacl)# permit 10.0.100.111 0.0.0.0


ArubaOS-Switch(config)# ip access-list standard std_pacl

ArubaOS-Switch(config-std-nacl)# permit 10.0.100.111/32


ArubaOS-Switch(config)# interface 4

ArubaOS-Switch(eth-4)# ip access-group 11 in

ArubaOS-Switch(eth-4)# ip access-group std_pacl in
```

Extended ACL

```
ArubaOS-Switch(config)# ip access-list extended 111

ArubaOS-Switch(config-ext-nacl)# deny ip 10.1.220.0 0.0.0.255 10.0.100.111 0.0.0.0

ArubaOS-Switch(config-ext-nacl)# permit ip any any


ArubaOS-Switch(config)# ip access-list extended ext_pacl

ArubaOS-Switch(config-ext-nacl)# deny ip 10.1.220.0/24 10.0.100.111/32

ArubaOS-Switch(config-ext-nacl)# permit ip any any


ArubaOS-Switch(config)# interface 4

ArubaOS-Switch(eth-4)# ip access-group 100 in

ArubaOS-Switch(eth-4)# ip access-group ext_pacl in
```

Comware

Basic ACL

```
[Comware]acl number 2011

[Comware-acl-basic-2011]rule permit source 10.0.100.111 0


[Comware]acl number 2012 name std_pacl

[Comware-acl-basic-2012-std_pacl]rule permit source 10.0.100.111 0


[Comware]interface g1/0/4

[Comware-GigabitEthernet1/0/4] packet-filter 2011 inbound

[Comware-GigabitEthernet1/0/4] packet-filter 2012 inbound
```

Advanced ACL

```
[Comware]acl number 3011

[Comware-acl-adv-3011]rule deny ip source 10.1.220.0 0.0.0.255 destination 10.0.100.111 0


[Comware]acl number 3012 name ext_pacl

[Comware-acl-adv-3012-ext_acl]rule deny ip source 10.1.220.0 0.0.0.255 destination
10.0.100.111 0

[Comware]interface g1/0/4

[Comware-GigabitEthernet1/0/4] packet-filter 3011 inbound

[Comware-GigabitEthernet1/0/4] packet-filter 3012 inbound
```

Cisco

Standard ACL

```
Cisco(config)#ip access-list standard 11

Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0


Cisco(config)#ip access-list standard std_pacl

Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0


Cisco(config)#interface g1/0/4

Cisco(config-if)#ip access-group 11 in

Cisco(config-if)#ip access-group std_pacl in
```

Extended ACL

```
Cisco(config)#ip access-list extended 121
Cisco(config-ext-nacl)#deny ip 10.1.220.0 0.0.0.255 10.0.100.111 0.0.0.0
Cisco(config-ext-nacl)#permit ip any any

Cisco(config)#ip access-list extended ext_pacl
Cisco(config-ext-nacl)#deny ip 10.1.220.0 255.255.255.0 10.0.100.111 255.255.255.255
Cisco(config-ext-nacl)#permit ip any any

Cisco(config)#interface g1/0/4
Cisco(config-if)#ip access-group 121 in
Cisco(config-if)#ip access-group ext_pacl in
```

Chapter 29 QoS

This chapter compares the commands you use to configure Quality of Service (QoS) on the ArubaOS-Switch, Comware, and Cisco operating systems.

A QoS network policy refers to the network-wide controls available to:

- Ensure uniform and efficient traffic handling throughout the network, while keeping the most important traffic moving at an acceptable speed, regardless of current bandwidth usage
- Exercise control over the priority settings of inbound traffic arriving in and traveling through the network

Adding bandwidth can be a good idea, but is not always feasible and does not completely eliminate the potential for network congestion. There will always be points in the network where multiple traffic streams merge or where network links change speed and capacity. The impact and number of these congestion points will increase over time as more applications and devices are added to the network.

When network congestion occurs, it is important to move traffic on the basis of relative importance. However, without QoS prioritization, less important traffic consumes network bandwidth and slows down or halts the delivery of more important traffic. Without QoS, most traffic that the switch receives is forwarded with the same priority it had upon entering the switch. In many cases, such traffic is normal priority and competes for bandwidth with all other normal-priority traffic, regardless of its relative importance to your organization's mission.

QoS Operational Characteristics

	ArubaOS-Switch	Comware	Cisco
QoS default	Enabled by default and operates based on 802.1p setting in packet	Enabled by default and operates based on 802.1p setting in packet	Disabled by default
Classification	Configured primarily on a global basis. Can be configured globally, on VLAN and on port	Configured per port or on VLAN with QoS policy	Configured per port or on SVI
Marking	Configured primarily on a global basis. Some configuration options can be set globally and some also set at VLAN or port	Configured globally, VLAN or port, using QoS policy	Configured per port or on SVI
Queue Scheduling	Configured per port	Configured per port	Configured per port or on SVI

a) QoS

ArubaOS-Switch	Comware	Cisco
		Cisco(config)#mls qos
	[Comware]interface g1/0/5	Cisco(config)#interface g1/0/5
	[Comware-GigabitEthernet1/0/5]qos trust dscp	Cisco(config-if)#mls qos trust dscp
ArubaOS-Switch(config)# qos type-of-service diff-services		Cisco(config)#mls qos map dscp-cos 0 8 16 24 32 40 48 56 to 0
ArubaOS-Switch(config)# interface 5	[Comware]interface g1/0/5	Cisco(config)#interface g1/0/5
ArubaOS-Switch(eth-5)# qos priority 6	[Comware-GigabitEthernet1/0/5]qos priority 6	Cisco(config-if)#mls qos cos 6
ArubaOS-Switch(config)# vlan 230	Step-1	
ArubaOS-Switch(vlan-230)# qos priority 6	[Comware]traffic classifier any	
	[Comware-classifier-any]if-match any	
	Step-2	
	[Comware]traffic behavior pri6	
	[Comware-behavior-pri6]remark dot1p 6	
	[Comware-behavior-pri6]accounting	
	Step-3	
	[Comware]qos policy any-pri6	
	[Comware-qospolicy-any-pri6]classifier any behavior pri6	
	Step-4	
	[Comware]qos vlan-policy any-pri6 vlan 230 inbound	
ArubaOS-Switch# show qos ?	[Comware]display qos ?	Cisco#show mls qos ?

ArubaOS-Switch

```
ArubaOS-Switch(config)# qos ?
udp-port                Configure UDP port-based priority.
 tcp-port                Configure TCP port-based priority.
 device-priority         Configure IP address-based traffic prioritization.
 dscp-map                Create a DSCP (Differentiated Services Codepoint) policy.
 protocol                Configure protocol-based traffic prioritization.
 queue-config            Configure port egress queue parameters.
 type-of-service         Configure DSCP-based traffic prioritization.

ArubaOS-Switch(config)# qos type-of-service ?
 diff-services           Prioritize IP packets based on their DSCP codepoint.
 ip-precedence           Prioritize IPv4 packets based on their ToS precedence.

ArubaOS-Switch(config)# qos type-of-service diff-services ?
```

```
 <000000-111111>       The DSCP codepoint in binary format.
 <0-63>                The DSCP codepoint in decimal format.
 af11
 af12
 af13
 af21
 af22
 af23
 af31
 af32
 af33
 af41
 af42
 af43
 ef
 cs0
 cs1
 cs2
 cs3
 cs4
 cs5
 cs6
 cs7
 <cr>

ArubaOS-Switch(config)# qos type-of-service diff-services


ArubaOS-Switch(config)# interface 5

ArubaOS-Switch(eth-5)# qos ?
 dscp                  Specify the DSCP policy to use.
 priority              Specify the 802.1p priority to use.

ArubaOS-Switch(eth-5)# qos priority ?
 0
 1
 2
 3
 4
 5
 6
 7

ArubaOS-Switch(eth-5)# qos priority 6


ArubaOS-Switch(config)# vlan 230

ArubaOS-Switch(vlan-230)# qos ?
 dscp                  Specify the DSCP policy to use.
 priority              Specify the 802.1p priority to use.

ArubaOS-Switch(vlan-230)# qos priority ?
 0
 1
 2
 3
 4
 5
 6
 7
```

```
ArubaOS-Switch(vlan-230)# qos priority 6


ArubaOS-Switch# show qos ?
 device-priority       Show IP address-based traffic prioritization settings.
 dscp-map              Show DSCP policy settings.
 port-priority         Show port-based prioritization settings.
 protocol-priority     Show protocol-based traffic prioritization settings.
 queue-config          Display port egress queue configuration information.
 resources             Show policy engine resource usage and availability.
 tcp-udp-port-priority Show TCP and UDP port-based prioritization settings.
 type-of-service       Show DSCP-based prioritization settings.
 vlan-priority         Show VLAN-based prioritization settings.
```

Comware5

```
[Comware5]interface g1/0/5

[Comware5-GigabitEthernet1/0/5]qos

[Comware5-GigabitEthernet1/0/5]qos ?
  apply      Apply specific QoS policy on interface
  bandwidth  Queue bandwidth
  gts        Apply GTS(Generic Traffic Shaping) policy on interface
  lr         Apply LR(Line Rate) policy on physical interface
  priority   Configure port priority
  sp         Configure Strict Priority(SP) queuing
  trust      Configure priority trust mode
  wfq        Configure Weighted Fair Queue(WFQ) queuing
  wred       Apply WRED(Weighted Random Early Detection) configuration
             information
  wrr        Configure Weighted Round Robin(WRR) queuing

[Comware5-GigabitEthernet1/0/5]qos trust ?
  dot1p  Trust 802.1p Precedence
  dscp   Differentiated Services Codepoint (DSCP)

[Comware5-GigabitEthernet1/0/6]qos trust dscp ?
  <cr>

[Comware5-GigabitEthernet1/0/6]qos trust dscp


[Comware5]interface g1/0/5

[Comware5-GigabitEthernet1/0/5]qos ?
  apply      Apply specific QoS policy on interface
  bandwidth  Queue bandwidth
  gts        Apply GTS(Generic Traffic Shaping) policy on interface
  lr         Apply LR(Line Rate) policy on physical interface
  priority   Configure port priority
  sp         Configure strict priority queue
  trust      Configure priority trust mode
  wfq        Configure weighted fair queue
  wred       Apply WRED(Weighted Random Early Detection) configuration
             information
  wrr        Configure weighted round robin queue

[Comware5-GigabitEthernet1/0/5]qos priority ?
  INTEGER<0-7>  Port priority value

[Comware5-GigabitEthernet1/0/5]qos priority 6 ?
  <cr>
```

```
[Comware5-GigabitEthernet1/0/5]qos priority 6
```

Step-1

```
[Comware5]traffic ?
  behavior    Specify traffic behavior
  classifier  Specify traffic classifier

[Comware5]traffic classifier ?
  STRING<1-31>  Name of classifier

[Comware5]traffic classifier any

[Comware5-classifier-any]?
Classifier view commands:
  cfd       Connectivity fault detection (IEEE 802.1ag)
  display   Display current system information
  if-match  Specify matching statement for classification
  mtracert  Trace route to multicast source
  ping      Ping function
  quit      Exit from current command view
  return    Exit to User View
  save      Save current configuration
  tracert   Trace route function
  undo      Cancel current setting

[Comware5-classifier-any]if-match ?
  acl               Specify ACL to match
  any               Specify any packets to match
  customer-dot1p    Specify IEEE 802.1p customer COS to match
  customer-vlan-id  Specify customer VLAN ID to match
  destination-mac   Specify destination MAC address to match
  dscp              Differentiated Services Codepoint (DSCP)
  ip-precedence     Specify IP precedence to match
  protocol          Specify protocol to match
  service-dot1p     Specify IEEE 802.1p service COS to match
  service-vlan-id   Specify service VLAN ID to match
  source-mac        Specify source MAC address to match
  system-index      Specify index of pre-defined matching rule

[Comware5-classifier-any]if-match any ?
  <cr>

[Comware5-classifier-any]if-match any
```

Step-2

```
[Comware5]traffic behavior ?
  STRING<1-31>  Name of behavior

[Comware5]traffic behavior pri6 ?
  <cr>

[Comware5]traffic behavior pri6

[Comware5-behavior-pri6]?
Behavior view commands:
  accounting  Specify Accounting feature
  car         Specify CAR (Committed Access Rate) feature
```

```
  cfd         Connectivity fault detection (IEEE 802.1ag)
  display     Display current system information
  filter      Specify packet filter feature
  mirror-to   Specify flow mirror feature
  mtracert    Trace route to multicast source
  nest        Nest top-most VLAN TAG or customer VLAN TAG
  ping        Ping function
  quit        Exit from current command view
  redirect    Specify Redirect feature
  remark      Remark QoS values of the packet
  return      Exit to User View
  save        Save current configuration
  tracert     Trace route function
  undo        Cancel current setting

[Comware5-behavior-pri6]remark ?
  customer-vlan-id  Remark Customer VLAN ID
  dot1p             Remark IEEE 802.1p COS
  drop-precedence   Remark drop precedence
  dscp              Differentiated Services Codepoint (DSCP)
  green             Specify type of remark for green packets
  ip-precedence     Remark IP precedence
  local-precedence  Remark local precedence
  red               Specify type of remark for red packets
  service-vlan-id   Remark service VLAN ID
  yellow            Specify type of remark for yellow packets

[Comware5-behavior-pri6]remark dot1p ?
  INTEGER<0-7>          Value of IEEE 802.1p COS
  customer-dot1p-trust  Copy the inner VLAN tag priority to outer VLAN tag
                        priority

[Comware5-behavior-pri6]remark dot1p 6 ?
  <cr>

[Comware5-behavior-pri6]remark dot1p 6

[Comware5-behavior-pri6]accounting ?
  <cr>

[Comware5-behavior-pri6]accounting
```

Step-3

```
[Comware5]qos policy ?
  STRING<1-31>  Name of QoS policy

[Comware5]qos policy any-pri6

[Comware5-qospolicy-any-pri6]?
Qospolicy view commands:
  cfd         Connectivity fault detection (IEEE 802.1ag)
  classifier  Specify the classifier to which policy relates
  display     Display current system information
  mtracert    Trace route to multicast source
  ping        Ping function
  quit        Exit from current command view
  return      Exit to User View
  save        Save current configuration
  tracert     Trace route function
  undo        Cancel current setting
```

```
[Comware5-qospolicy-any-pri6]classifier ?
  STRING<1-31>  Name of classifier

[Comware5-qospolicy-any-pri6]classifier any ?
  behavior  Specify traffic behavior

[Comware5-qospolicy-any-pri6]classifier any behavior ?
  STRING<1-31>  Name of behavior

[Comware5-qospolicy-any-pri6]classifier any behavior pri6 ?
  mode  Specify the classifier-behavior mode
  <cr>

[Comware5-qospolicy-any-pri6]classifier any behavior pri6
```

Step-4

```
[Comware5]qos vlan-policy ?
  STRING<1-31>  Specify qos policy name

[Comware5]qos vlan-policy any-pri6 ?
  vlan  Apply qos policy on vlan

[Comware5]qos vlan-policy any-pri6 vlan ?
  INTEGER<1-4094>  Specify vlan id

[Comware5]qos vlan-policy any-pri6 vlan 230 ?
  INTEGER<1-4094>  Specify vlan id
  inbound          Assign policy to the inbound of a vlan
  outbound         Assign policy to the outbound of a vlan
  to               Range of vlan id

[Comware5]qos vlan-policy any-pri6 vlan 230 inbound ?
  <cr>

[Comware5]qos vlan-policy any-pri6 vlan 230 inbound


[Comware5]display qos ?
  gts          GTS(Generic Traffic Shaping) policy on interface
  lr           LR(Line Rate) policy on physical interface
  map-table    Priority map table configuration information
  policy       QoS policy configuration information
  sp           SP(strict priority queue) on port
  trust        Priority trust information
  vlan-policy  Vlan-policy configuration information
  wfq          Hardware WFQ(hardware weighted fair queue) on port
  wred         WRED(Weighted Random Early Detect) on interface
  wrr          WRR(weighted round robin queue) on port
```

Comware7

```
[Comware7]interface g1/0/5

[Comware7-GigabitEthernet1/0/5]qos

[Comware-GigabitEthernet1/0/5]qos ?
  apply      Apply specific QoS policy on interface
  bandwidth  Set the queue bandwidth
  gts        Configure Generic Traffic Shaping (GTS)
  lr         Configure Line Rate (LR)
  priority   Configure port priority
```

```
  sp         Configure Strict Priority (SP) queuing
  trust      Configure priority trust mode
  wfq        Configure Weighted Fair Queuing (WFQ)
  wred       Configure Weighted Random Early Detection (WRED)
  wrr        Configure Weighted Round Robin (WRR) queuing

[Comware7-GigabitEthernet1/0/5]qos trust ?
  dot1p  802.1p priority
  dscp   DSCP

[Comware7-GigabitEthernet1/0/6]qos trust dscp ?
  <cr>

[Comware7-GigabitEthernet1/0/6]qos trust dscp


[Comware7]interface g1/0/5

[Comware7-GigabitEthernet1/0/5]qos ?
  apply      Apply specific QoS policy on interface
  bandwidth  Set the queue bandwidth
  gts        Configure Generic Traffic Shaping (GTS)
  lr         Configure Line Rate (LR)
  priority   Configure port priority
  sp         Configure Strict Priority (SP) queuing
  trust      Configure priority trust mode
  wfq        Configure Weighted Fair Queuing (WFQ)
  wred       Configure Weighted Random Early Detection (WRED)
  wrr        Configure Weighted Round Robin (WRR) queuing

[Comware7-GigabitEthernet1/0/5]qos priority ?
  INTEGER<0-7>  Port priority value

[Comware7-GigabitEthernet1/0/5]qos priority 6 ?
  <cr>

[Comware7-GigabitEthernet1/0/5]qos priority 6
```

Step-1

```
[Comware7]traffic ?
  behavior    Specify traffic behavior
  classifier  Specify traffic classifier

[Comware7]traffic classifier ?
  STRING<1-31>  Name of classifier

[Comware7]traffic classifier any

[Comware7-classifier-any]?
Classifier view commands:
  cfd                 Connectivity Fault Detection (CFD) module
  diagnostic-logfile  Diagnostic log file configuration
  display             Display current system information
  if-match            Specify a match criterion for classifier
  logfile             Log file configuration
  monitor             System monitor
  ping                Ping function
  quit                Exit from current command view
  return              Exit to User View
  save                Save current configuration
  security-logfile    Security log file configuration
```

```
  tracert              Tracert function
  undo                 Cancel current setting

[Comware7-classifier-any]if-match ?
  acl                Specify ACL to match
  any                Specify any packets to match
  control-plane      Specify control plane pre-defined matching rule
  customer-dot1p     Specify customer 802.1p priority to match
  customer-vlan-id   Specify customer VLAN ID to match
  destination-mac    Specify destination MAC address to match
  dscp               Specify DSCP to match
  ip-precedence      Specify IP precedence to match
  protocol           Specify protocol to match
  qos-local-id       Specify QoS local ID to match
  service-dot1p      Specify service 802.1p priority to match
  service-vlan-id    Specify service VLAN ID to match
  source-mac         Specify source MAC address to match

[Comware7-classifier-any]if-match any ?
  <cr>

[Comware7-classifier-any]if-match any
```

Step-2

```
[Comware7]traffic behavior ?
  STRING<1-31>  Name of behavior

[Comware7]traffic behavior pri6

[Comware7-behavior-pri6]?
Behavior view commands:
  accounting           Specify accounting function
  car                  Configure Committed Access Rate (CAR)
  cfd                  Connectivity Fault Detection (CFD) module
  diagnostic-logfile   Diagnostic log file configuration
  display              Display current system information
  filter               Specify packet filtering function
  logfile              Log file configuration
  mirror-to            Specify traffic mirroring function
  monitor              System monitor
  nest                 Nest VLAN tag
  ping                 Ping function
  quit                 Exit from current command view
  redirect             Specify redirecting function
  remark               Specify marking function
  return               Exit to User View
  save                 Save current configuration
  security-logfile     Security log file configuration
  tracert              Tracert function
  undo                 Cancel current setting

[Comware7-behavior-pri6]remark ?
  customer-vlan-id   Remark customer VLAN ID
  dot1p              Remark 802.1p priority
  drop-precedence    Remark drop precedence
  dscp               Remark DSCP
  green              Specify green packets
  ip-precedence      Remark IP precedence
  local-precedence   Remark local precedence
  qos-local-id       Remark QoS local ID
  red                Specify red packets
```

```
  service-vlan-id   Remark service VLAN ID
  yellow            Specify yellow packets

[Comware7-behavior-pri6]remark dot1p ?
  INTEGER<0-7>          Value of IEEE 802.1p COS
  customer-dot1p-trust  Copy the inner VLAN tag priority to outer VLAN tag
                        priority

[Comware7-behavior-pri6]remark dot1p 6 ?
  <cr>

[Comware7-behavior-pri6]remark dot1p 6

[Comware7-behavior-pri6]accounting ?
  byte    Accounting in bytes
  packet  Accounting in packets

[Comware7-behavior-pri6]accounting packet ?
  <cr>

[Comware7-behavior-pri6]accounting packet
```

Step-3

```
[Comware7]qos policy ?
  STRING<1-31>  Policy name

[Comware7]qos policy any-pri6

[Comware7-qospolicy-any-pri6]?
Qospolicy view commands:
  cfd                 Connectivity Fault Detection (CFD) module
  classifier          Specify the classifier to which policy relates
  diagnostic-logfile  Diagnostic log file configuration
  display             Display current system information
  logfile             Log file configuration
  monitor             System monitor
  ping                Ping function
  quit                Exit from current command view
  return              Exit to User View
  save                Save current configuration
  security-logfile    Security log file configuration
  tracert             Tracert function
  undo                Cancel current setting

[Comware7-qospolicy-any-pri6]classifier ?
  STRING<1-31>  Name of classifier

[Comware7-qospolicy-any-pri6]classifier any ?
  behavior  Specify traffic behavior

[Comware7-qospolicy-any-pri6]classifier any behavior ?
  STRING<1-31>  Name of behavior

[Comware7-qospolicy-any-pri6]classifier any behavior pri6 ?
  insert-before  Insert this classifier before another classifier
  mode           Specify the classifier-behavior mode
  <cr>

[Comware7-qospolicy-any-pri6]classifier any behavior pri6
```

Step-4

```
[Comware7]qos vlan-policy ?
  STRING<1-31>  Policy name

[Comware7]qos vlan-policy any-pri6 ?
  vlan  Apply QoS policy on VLAN

[Comware7]qos vlan-policy any-pri6 vlan ?
  INTEGER<1-4094>  VLAN ID

[Comware7]qos vlan-policy any-pri6 vlan 230 ?
  INTEGER<1-4094>  VLAN ID
  inbound          Inbound direction
  outbound         Outbound direction
  to               Range of VLAN ID

[Comware7]qos vlan-policy any-pri6 vlan 230 inbound ?
  <cr>

[Comware7]qos vlan-policy any-pri6 vlan 230 inbound


[Comware7]display qos ?
  car               Committed Access Rate (CAR) information
  gts               Generic Traffic Shaping (GTS) information
  lr                Line Rate (LR) information
  map-table         Priority mapping table information
  policy            QoS policy information
  qmprofile         Queue management profile information
  queue             Queue information
  queue-statistics  Port queue statistics
  trust             Priority trust mode and port priority information
  vlan-policy       Apply a QoS policy to VLANs information
  wred              Weighted Random Early Detection (WRED) information
```

Cisco

```
Cisco(config)#mls qos ?
  aggregate-policer  Named aggregate policer
  map                qos map keyword
  queue-set          Choose a queue set for this queue
  rewrite            Rewrite Packet/Frame
  srr-queue          Configure SRR receive queues
  <cr>

Cisco(config)#mls qos


Cisco(config)#interface g1/0/5

Cisco(config-if)#mls qos ?
  cos            cos keyword
  dscp-mutation  dscp-mutation keyword
  ipe            ipe keyword
  trust          trust keyword
  vlan-based     vlan-based keyword

Cisco(config-if)#mls qos trust ?
  cos            cos keyword
  device         trusted device class
  dscp           dscp keyword
  ip-precedence  ip-precedence keyword
```

```
  <cr>

Cisco(config-if)#mls qos trust dscp ?
  <cr>

Cisco(config-if)#mls qos trust dscp


Cisco(config)#mls qos map ?
  cos-dscp       cos-dscp map: eight dscp values for cos 0-7
  dscp-cos       dscp-cos map keyword
  dscp-mutation  dscp-mutation map keyword
  ip-prec-dscp   dscp values for ip precedences 0 - 7
  policed-dscp   policed-dscp map keyword

Cisco(config)#mls qos map dscp-cos ?
  <0-63>  DSCP values separated by spaces (up to 8 values total)

Cisco(config)#mls qos map dscp-cos 0 8 16 24 32 40 48 56 ?
  to  to keyword

Cisco(config)#mls qos map dscp-cos 0 8 16 24 32 40 48 56 to ?
  <0-7>  cos value

Cisco(config)#mls qos map dscp-cos 0 8 16 24 32 40 48 56 to 0 ?
  <cr>

Cisco(config)#mls qos map dscp-cos 0 8 16 24 32 40 48 56 to 0


Cisco(config)#interface g1/0/5

Cisco(config-if)#mls qos ?
  cos            cos keyword
  dscp-mutation  dscp-mutation keyword
  ipe            ipe keyword
  trust          trust keyword
  vlan-based     vlan-based keyword


Cisco(config-if)#mls qos cos ?
  <0-7>     class of service value between 0 and 7
  override  override keyword

Cisco(config-if)#mls qos cos 6


Cisco#show mls qos ?
  aggregate-policer  aggregate-policer keyword
  input-queue        input-queue keyword
  interface          interface keyword
  maps               maps keyword
  queue-set          queue-set keyword
  vlan               VLAN keyword
  |                  Output modifiers
  <cr>
```

b) Rate Limiting

ArubaOS-Switch	Comware5	Cisco
ingress	Note: ingress rate limiting not an available feature	ingress
ArubaOS-Switch(config)# interface 7		step-1
ArubaOS-Switch(eth-7)# rate-limit all in percent 10		Cisco(config)#ip access-list extended 130
		Cisco(config-ext-nacl)#permit ip any any
		step-2
		Cisco(config)#class-map all_traffic
		Cisco(config-cmap)#match access-group 130
		step-3
		Cisco(config)#policy-map rate_limit
		Cisco(config-pmap)#class all_traffic
		Cisco(config-pmap-c)#police 10000000 8000 exceed-action drop
		step-4
		Cisco(config)#interface g1/0/7
		Cisco(config-if)#service-policy input rate_limit
egress	egress	egress
ArubaOS-Switch(config)# interface 8	[Comware5]interface g1/0/8	Cisco(config)#interface g1/0/8
ArubaOS-Switch(eth-8)# rate-limit all out kbps 10000	[Comware5-GigabitEthernet1/0/8]qos lr outbound cir 10048	Cisco(config-if)#srr-queue bandwidth limit 10
	Comware7	
	ingress	
	[Comware7]interface g1/0/7	
	[Comware7-GigabitEthernet1/0/7]qos lr inbound cir 10048	
	egress	
	[Comware7]interface g1/0/8	
	[Comware7-GigabitEthernet1/0/8]qos lr outbound cir 10048	

ArubaOS-Switch

ingress

```
ArubaOS-Switch(config)# interface 7

ArubaOS-Switch(eth-7)# rate-limit ?
all                    Set rate limits for all traffic.
```

```
 bcast                  Set rate limits for broadcast traffic.
 icmp                   Set rate limits for incoming ICMP traffic.
 mcast                  Set rate limits for multicast traffic.

ArubaOS-Switch(eth-7)# rate-limit all ?
 in                     Set rate limits for all incoming traffic.
 out                    Set rate limits for all outgoing traffic.

ArubaOS-Switch(eth-7)# rate-limit all in ?
 kbps                   Set the rate limit in kilobits per second.
 percent                Set the rate limit as a percentage of the port link speed.

ArubaOS-Switch(eth-7)# rate-limit all in percent ?
 <0-100>                Enter an integer number.

ArubaOS-Switch(eth-7)# rate-limit all in percent 10 ?
 <cr>

ArubaOS-Switch(eth-7)# rate-limit all in percent 10
```

egress

```
ArubaOS-Switch(config)# interface 8

ArubaOS-Switch(eth-8)# rate-limit all out ?
 kbps                   Set the rate limit in kilobits per second.
 percent                Set the rate limit as a percentage of the port link speed.

ArubaOS-Switch(eth-8)# rate-limit all out kbps ?
 <0-10000000>           Enter an integer number.

ArubaOS-Switch(eth-8)# rate-limit all out kbps 10000 ?
 <cr>

ArubaOS-Switch(eth-8)# rate-limit all out kbps 10000
```

Comware5

Note: ingress rate limiting not an available feature

egress

```
[Comware5]interface g1/0/8

[Comware5-GigabitEthernet1/0/8]qos ?
  apply      Apply specific QoS policy on interface
  bandwidth  Queue bandwidth
  gts        Apply GTS(Generic Traffic Shaping) policy on interface
  lr         Apply LR(Line Rate) policy on physical interface
  priority   Configure port priority
  sp         Configure Strict Priority(SP) queuing
  trust      Configure priority trust mode
  wfq        Configure Weighted Fair Queue(WFQ) queuing
  wred       Apply WRED(Weighted Random Early Detection) configuration
             information
  wrr        Configure Weighted Round Robin(WRR) queuing

[Comware5-GigabitEthernet1/0/8]qos lr ?
  outbound  Limit the rate on outbound

[Comware5-GigabitEthernet1/0/8]qos lr outbound ?
```

```
  cir  Target rate of physical interface(kbps)

[Comware5-GigabitEthernet1/0/8]qos lr outbound cir ?
  INTEGER<64-1000000>  Committed Information Rate(kbps), it must be a multiple
                       of 64

[Comware5-GigabitEthernet1/0/8]qos lr outbound cir 10048 ?
  cbs   Committed Burst Size (byte)
  <cr>

[Comware5-GigabitEthernet1/0/8]qos lr outbound cir 10048
```

Comware7

ingress

```
[Comware7]interface g1/0/7
[Comware7-GigabitEthernet1/0/7]qos ?
  apply      Apply specific QoS policy on interface
  bandwidth  Set the queue bandwidth
  gts        Configure Generic Traffic Shaping (GTS)
  lr         Configure Line Rate (LR)
  priority   Configure port priority
  sp         Configure Strict Priority (SP) queuing
  trust      Configure priority trust mode
  wfq        Configure Weighted Fair Queuing (WFQ)
  wred       Configure Weighted Random Early Detection (WRED)
  wrr        Configure Weighted Round Robin (WRR) queuing

[Comware7-GigabitEthernet1/0/7]qos lr ?
  inbound   Limit the rate on the inbound direction
  outbound  Limit the rate on the outbound direction

[Comware7-GigabitEthernet1/0/7]qos lr inbound ?
  cir  Specify Committed Information Rate (CIR)

[Comware7-GigabitEthernet1/0/7]qos lr inbound cir ?
  INTEGER<8-1048576>  Value of CIR in kbps, it must be a multiple of 8

[Comware7-GigabitEthernet1/0/7]qos lr inbound cir 10048 ?
  cbs   Specify Committed Burst Size (CBS)
  <cr>

[Comware7-GigabitEthernet1/0/7]qos lr inbound cir 10048
```

egress

```
[Comware7]interface g1/0/8

[Comware7-GigabitEthernet1/0/8]qos ?

[Comware7-GigabitEthernet1/0/8]qos lr outbound ?
  cir  Target rate of physical interface(kbps)

[Comware7-GigabitEthernet1/0/8]qos lr outbound cir ?
  INTEGER<8-1048576>  Value of CIR in kbps, it must be a multiple of 8

[Comware7-GigabitEthernet1/0/8]qos lr outbound cir 10048 ?
  cbs   Committed Burst Size (byte)
  <cr>

[Comware7-GigabitEthernet1/0/8]qos lr outbound cir 10048
```

Cisco

ingress

step-1

```
Cisco(config)#ip access-list extended 130

Cisco(config-ext-nacl)#permit ip any any
```

step-2

```
Cisco(config)#class-map ?

  WORD       class-map name
  match-all  Logical-AND all matching statements under this classmap
  match-any  Logical-OR all matching statements under this classmap
  type       Configure CPL Class Map

Cisco(config)#class-map all_traffic ?
  <cr>

Cisco(config)#class-map all_traffic

Cisco(config-cmap)#?

Class-map configuration commands:

  description  Class-Map description
  exit         Exit from class-map configuration mode
  match        classification criteria
  no           Negate or set default values of a command

Cisco(config-cmap)#match ?

  access-group     Access group
  input-interface  Select an input interface to match
  ip               IP specific values

Cisco(config-cmap)#match access-group ?

  <1-2799>  Access list index

  name      Named Access List

Cisco(config-cmap)#match access-group 130
```

step-3

```
Cisco(config)#policy-map ?

  WORD  policy-map name

  type  type of the policy-map

Cisco(config)#policy-map rate_limit ?
  <cr>

Cisco(config)#policy-map rate_limit

Cisco(config-pmap)#class ?
```

```
  WORD            class-map name

  class-default   System default class matching otherwise unclassified packets

Cisco(config-pmap)#class all_traffic ?

  fragment          configure qos fragment class

  service-fragment  configure qos service-fragment class

  <cr>

Cisco(config-pmap)#class all_traffic

Cisco(config-pmap-c)#police ?

  <8000-10000000000>  Bits per second (postfix k, m, g optional; decimal point
                      allowed)
  aggregate           Choose aggregate policer for current class

Cisco(config-pmap-c)#police 10000000 ?

  <8000-1000000>  Normal burst bytes

Cisco(config-pmap-c)#police 10000000 8000 ?

  exceed-action  action when rate is exceeded
  <cr>


Cisco(config-pmap-c)#police 10000000 8000 exceed-action ?

  drop                    drop packet
  policed-dscp-transmit  change dscp per policed-dscp map and send it

Cisco(config-pmap-c)#police 10000000 8000 exceed-action drop ?
  <cr>

Cisco(config-pmap-c)#police 10000000 8000 exceed-action drop
```

step-4

```
Cisco(config)#interface g1/0/7

Cisco(config-if)#service-policy ?

  input   Assign policy-map to the input of an interface
  output  Assign policy-map to the output of an interface
  type    Configure CPL Service Policy

Cisco(config-if)#service-policy input ?

  WORD  policy-map name

Cisco(config-if)#service-policy input rate_limit ?
  <cr>

Cisco(config-if)#service-policy input rate_limit
```

egress

```
Cisco(config)#interface g1/0/8

Cisco(config-if)#srr-queue ?

  bandwidth  Configure shared bandwidth

Cisco(config-if)#srr-queue bandwidth ?
  limit  Configure bandwidth-limit for this interface

  shape  Configure shaping on transmit queues

  share  Configure shared bandwidth

Cisco(config-if)#srr-queue bandwidth limit ?

  <10-90>  enter bandwidth limit for interface as percentage


Cisco(config-if)#srr-queue bandwidth limit 10 ?
  <cr>

Cisco(config-if)#srr-queue bandwidth limit 10
```

Chapter 30 IP Multicast

This chapter compares the commands you use to configure Protocol Independent Multicast Dense Mode (PIM-DM) and PIM Sparse Mode (PIM-SM). It also covers Internet Group Management Protocol (IGMP).

PIM provides IP multicast forwarding by leveraging the static routes or unicast routing tables that any unicast routing protocol generates, such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), or Border Gateway Protocol (BGP). You can implement multicast routing independent of the unicast routing protocols running on the device, as long as the corresponding multicast routing entries are created through unicast routes. PIM uses the reverse path forwarding (RPF) mechanism to implement multicast forwarding. When a multicast packet arrives on an interface of the device, it is subject to an RPF check. If the RPF check succeeds, the device creates the corresponding routing entry and forwards the packet. If the RPF check fails, the device discards the packet.

In a network that transmits IP multicast traffic for multimedia applications, such traffic is blocked at routed interface (VLAN) boundaries unless a multicast routing protocol is running. PIM is a family of routing protocols that forms multicast trees to forward traffic from multicast sources to subnets that have used a protocol such as Internet Group Management Protocol (IGMP) to request the traffic. PIM relies on the unicast routing tables that any of several unicast routing protocols use to identify the path back to a multicast source (RPF). With this information, PIM sets up the distribution tree for the multicast traffic. The PIM-DM and PIM-SM protocols on the switches covered in this chapter enable and control multicast traffic routing.

IGMP provides the multicast traffic link between a host and a multicast router running PIM-DM or PIM-SM. You must enable IGMP and either PIM-DM or PIM-SM on VLANs whose member ports have directly connected hosts with a valid need to join multicast groups.

You use PIM-DM in networks where, at any given time, multicast group members exist in relatively large numbers and are present in most subnets.

You use PIM-SM in networks where multicast sources and group members are sparsely distributed over a wide area and can result in unnecessary multicast traffic on routers outside the distribution paths needed for traffic between a given multicast source and the hosts belonging to the multicast group. In such networks, PIM-SM can reduce the effect of multicast traffic flows in network areas where they are not needed. And because PIM-SM does not automatically flood traffic, it is a logical choice in lower bandwidth situations such as WAN environments.

a) PIM Dense

ArubaOS-Switch	Comware5	Cisco
ArubaOS-Switch(config)# ip multicast-routing	[Comware5]multicast routing-enable	Cisco(config)#ip multicast-routing distributed
ArubaOS-Switch(config)# router pim ArubaOS-Switch(pim)# enable		
ArubaOS-Switch(pim)# vlan 220	[Comware5]interface Vlan-interface 220	Cisco(config)#interface vlan 220
ArubaOS-Switch(vlan-220)# ip pim-dense	[Comware5-Vlan-interface220]pim dm	Cisco(config-if)#ip pim dense-mode
ArubaOS-Switch# show ip pim ?	[Comware5]display pim ?	Cisco#show ip pim ?
ArubaOS-Switch# show ip mroute ?	[Comware5]display multicast routing-table ?	Cisco#show ip mroute ?
	Comware7	
	[Comware7]multicast routing	
	[Comware7]interface Vlan-interface 220	
	[Comware7-Vlan-interface220]pim dm	
	[Comware7]display pim ?	
	[Comware7]display multicast routing-table ?	

ArubaOS-Switch

```
ArubaOS-Switch(config)# ip multicast-routing

ArubaOS-Switch(config)# router pim

ArubaOS-Switch(pim)# enable


ArubaOS-Switch(pim)# vlan 220

ArubaOS-Switch(vlan-220)# ip pim-dense ?
 graft-retry-interval  Set the interval a PIM router waits for a Graft Ack before
                       resending a Graft on this interface.
 hello-delay           Set the maximum time before a triggered PIM Hello message is
                       transmitted on this interface.
 hello-interval        Set the frequency at which PIM Hello messages are transmitted on
                       this interface.
 ip-addr               Set the source IP address for the PIM-DM packets sent out on this
                       interface.
 lan-prune-delay       Turn on/off the LAN Prune Delay Option on this interface.
 max-graft-retries     Set the maximum number of times this router will resend a Graft on
                       this interface.
 override-interval     Set the value inserted into the Override Interval field of a LAN
                       Prune Delay option on this interface.
 propagation-delay     Set the value inserted into the LAN Prune Delay field of a LAN
                       Prune Delay option on this interface.
```

```
 ttl-threshold          Set the Time To Live in a PIM-DM State Refresh message at which it
                        is not forwarded on this interface.
 <cr>

ArubaOS-Switch(vlan-220)# ip pim-dense


ArubaOS-Switch# show ip pim ?
 bsr                    Show Bootstrap Router information.
 interface              Show PIM interface information.
 mroute                 Show PIM-specific information from the IP multicast routing table.
 neighbor               Show PIM neighbor information.
 pending                Show (*,G) and (S,G) Join Pending Information.
 rp-candidate           Show Candidate-RP operational and configuration information.
 rp-set                 Show RP-Set information available on the router.
 rpf-override           Show the PIM RPF override entries.
 <cr>


ArubaOS-Switch# show ip mroute ?
 interface              Show IP multicast routing interfaces' information.
 IP-ADDR                Show detailed information for the specified entry from the IP
                        multicast routing table.
 <cr>
```

Comware5

```
[Comware5]multicast routing-enable


[Comware5]interface Vlan-interface 220

[Comware5-Vlan-interface220]pim ?
  bfd                     Enable BFD for PIM on interface
  bsr-boundary            Bootstrap router boundary
  dm                      Enable PIM dense mode
  hello-option            Specify hello option
  holdtime                Specify holdtime
  ipv6                    PIM IPv6 status and configuration information
  neighbor-policy         Policy to accept PIM hello messages
  require-genid           Require generation id
  sm                      Enable PIM sparse/SSM mode
  state-refresh-capable   State-refresh capability
  timer                   Specify PIM timer
  triggered-hello-delay   Triggered hello delay

[Comware5-Vlan-interface220]pim dm ?
  <cr>

[Comware5-Vlan-interface220]pim dm


[Comware5]display pim ?
  all-instance     All vpn-instances
  bsr-info         Bootstrap router information
  claimed-route    PIM claim route information
  control-message  PIM control message information
  df-info          Designated forwarder information of bidirectional PIM
  grafts           PIM unacknowledged grafts' information
  interface        PIM-enabled interface
  ipv6             PIM IPv6 status and configuration information
  join-prune       PIM join prune queue
  neighbor         PIM neighbor information
  routing-table    PIM routing table
```

```
  rp-info          RP information
  vpn-instance     Specify vpn-instance


[Comware5]display multicast routing-table ?
  X.X.X.X             Group address
  X.X.X.X             Source address
  all-instance        All vpn-instances
  incoming-interface  Incoming interface
  outgoing-interface  Outgoing interface
  static              Static configuration
  vpn-instance        VPN instance
  |                   Matching output
  <cr>
```

Comware7

```
[Comware7]multicast routing


[Comware7]interface Vlan-interface 220

[Comware7-Vlan-interface220]pim ?
  bfd                     Enable BFD for PIM
  bsr-boundary            Specify Bootstrap Router (BSR) message boundary
  dm                      Enable Dense Mode (DM)
  hello-option            Specify hello option
  holdtime                Specify holdtime timer
  neighbor-policy         Specify a legal source address range for hello messages
  passive                 Enable passive capability
  require-genid           Require generation ID in hello messages
  sm                      Enable Sparse Mode (SM)
  state-refresh-capable   Enable state refresh capability
  timer                   Specify a timer
  triggered-hello-delay   Specify the maximum delay between two hello messages

[Comware7-Vlan-interface220]pim dm ?
  <cr>

[Comware7-Vlan-interface220]pim dm


[Comware7]display pim ?
  bsr-info       Display Bootstrap Router (BSR) information
  c-rp           Display Candidate-RP (C-RP) information
  claimed-route  Display information about all routes that PIM uses
  df-info        Display Designated Forwarder (DF) information
  interface      Display PIM information on an interface
  neighbor       Display PIM neighbor information
  routing-table  Display PIM routing table information
  rp-info        Display Rendezvous Point (RP) information
  statistics     Display PIM packet statistics information
  vpn-instance   Specify a VPN instance


[Comware7]display multicast routing-table ?
  >                   Redirect it to a file
  >>                  Redirect it to a file in append mode
  X.X.X.X             Group address
  X.X.X.X             Source address
  incoming-interface  Specify incoming interface in entries
  outgoing-interface  Specify outgoing interface in entries
  static              Static information
  |                   Matching output
```

```
  <cr>
```

Cisco

```
Cisco(config)#ip multicast-routing distributed

Cisco(config)#interface vlan 220

Cisco(config-if)#ip pim ?
  bidir-neighbor-filter  PIM bidir capable peering filter
  bsr-border             Border of PIM domain
  dense-mode             Enable PIM dense-mode operation
  dr-priority            PIM router DR priority
  nbma-mode              Use Non-Broadcast Multi-Access (NBMA) mode on
                         interface
  neighbor-filter        PIM peering filter
  passive                Enable PIM passive interface operation
  query-interval         PIM router query interval
  sparse-dense-mode      Enable PIM sparse-dense-mode operation
  sparse-mode            Enable PIM sparse-mode operation
  state-refresh          PIM DM State-Refresh configuration

Cisco(config-if)#ip pim dense-mode

Cisco#show ip pim ?
  autorp      Global AutoRP information
  boundary    debug boundary comand
  bsr-router  Bootstrap router (v2)
  interface   PIM interface information
  mdt         Multicast tunnel information
  neighbor    PIM neighbor information
  rp          PIM Rendezvous Point (RP) information
  rp-hash     RP to be chosen based on group selected
  vrf         Select VPN Routing/Forwarding instance


Cisco#show ip mroute ?
  Hostname or A.B.C.D  Source or group IP name or address
  active               Active multicast sources
  bidirectional        Show bidirectional multicast routes
  count                Route and packet count data
  dense                Show dense multicast routes
  interface            Interface information
  proxy                List proxies
  pruned               Pruned routes
  sparse               Show sparse multicast routes
  ssm                  show SSM multicast routes
  static               Static multicast routes
  summary              Provide abbreviated display
  verbose              Verbose
  vrf                  Select VPN Routing/Forwarding instance
  |                    Output modifiers
  <cr>
```

b) PIM Sparse

ArubaOS-Switch	Comware5	Cisco
ArubaOS-Switch(config)# ip multicast-routing	[Comware5]multicast routing-enable	Cisco(config)#ip multicast-routing distributed
ArubaOS-Switch(config)# router pim		

ArubaOS-Switch(pim)# enable		
ArubaOS-Switch(pim)# vlan 220 ArubaOS-Switch(vlan-220)# ip pim-sparse ArubaOS-Switch(vlan-220)# router pim	[Comware5]interface Vlan-interface 220 [Comware5-Vlan-interface220]pim sm	Cisco(config)#interface vlan 220 Cisco(config-if)#ip pim sparse-mode Cisco(config-if)#exit
ArubaOS-Switch(pim)# rp-address 10.1.220.1	[Comware5-Vlan-interface220]pim [Comware5-pim]static-rp 10.1.220.1	Cisco(config)#ip pim rp-address 10.1.220.1
ArubaOS-Switch(pim)# rp-candidate source-ip-vlan 220	[Comware5-pim]c-rp Vlan-interface 220	Cisco(config)#ip pim rp-candidate vlan 220
ArubaOS-Switch(pim)# bsr-candidate source-ip-vlan 220	[Comware5-pim]c-bsr Vlan-interface 220	Cisco(config)#ip pim bsr-candidate vlan 220
ArubaOS-Switch# show ip pim ?	[Comware5]display pim ?	Cisco#show ip pim ?
ArubaOS-Switch# show ip mroute ?	[Comware5]display multicast routing-table ?	Cisco#show ip mroute ?
	Comware7	
	[Comware7]multicast routing	
	[Comware7]interface Vlan-interface 220 [Comware7-Vlan-interface220]pim sm	
	[Comware7-Vlan-interface220]pim [Comware7-pim]static-rp 10.1.220.1	
	[Comware7-pim]c-rp 10.1.220.1	
	[Comware7-pim]c-bsr 10.1.220.1	
	[Comware7]display pim ?	
	[Comware7]display multicast routing-table ?	

ArubaOS-Switch

```
ArubaOS-Switch(config)# ip multicast-routing


ArubaOS-Switch(config)# router pim

ArubaOS-Switch(pim)# enable


ArubaOS-Switch(config)# vlan 220

ArubaOS-Switch(vlan-220)# ip pim-sparse ?
```

```
 dr-priority           Set the priority value to use on the interface in the Designated
                       Router election process.
 hello-delay           Set the maximum time before a triggered PIM Hello message is
                       transmitted on this interface.
 hello-interval        Set the frequency at which PIM Hello messages are transmitted on
                       this interface.
 ip-addr               Set the source IP address for the PIM-SM packets sent out on this
                       interface.
 lan-prune-delay       Turn on/off the LAN Prune Delay Option on this interface.
 override-interval     Set the value inserted into the Override Interval field of a LAN
                       Prune Delay option on this interface.
 propagation-delay     Set the value inserted into the LAN Prune Delay field of a LAN
                       Prune Delay option on this interface.
 <cr>

ArubaOS-Switch(vlan-220)# ip pim-sparse


ArubaOS-Switch(vlan-220-pim-sparse)# router pim

ArubaOS-Switch(pim)# ?
 bsr-candidate         Configure the router to advertise itself as the Candidate
                       Bootstrap Router (Candidate-BSR) for a PIM-SM domain.
 disable               Disable PIM globally.
 enable                Enable PIM globally.
 join-prune-interval   Configure interval at which the router will send periodic PIM-SM
                       Join/Prune messages.
 rp-address            Statically configure the Rendezvous Point (RP) to accept
                       multicast traffic for specified group or range of groups.
 rp-candidate          Configure router to advertise itself as the Candidate Rendezvous
                       Point (Candidate-RP) to the Bootstrap Router (BSR).
 rpf-override          Add, edit or delete RPF override entries.
 spt-threshold         Specify whether switching to the Shortest Path Tree is enabled or
                       disabled on the router.
 state-refresh         Set the interval between successive State Refresh messages
                       originated by this router.
 trap                  Enable/disable PIM traps.

ArubaOS-Switch(pim)# rp-address 10.1.220.1
 GROUP-ADDR/GROUP-MASK Specify the range of multicast group addresses associated with the
                       static RP.
 <cr>

ArubaOS-Switch(pim)# rp-address 10.1.220.1

ArubaOS-Switch(pim)# rp-candidate source-ip-vlan ?
 VLAN-ID               Enter a VLAN identifier or a VLAN name.

ArubaOS-Switch(pim)# rp-candidate source-ip-vlan 220

ArubaOS-Switch(pim)# bsr-candidate ?
 bsm-interval          Specify the interval for sending Bootstrap messages on PIM-SM
                       interfaces.
 hash-mask-length      Specify the length (in bits) of the hash mask.
 priority              Specify the priority for the Candidate Bootstrap router.
 source-ip-vlan        Specify the VLAN to use as a source for Candidate-BSR router IP
                       address(PIM-SM must be enabled on this VLAN).
 <cr>
ArubaOS-Switch(pim)# bsr-candidate source-ip-vlan 220


ArubaOS-Switch# show ip pim ?
bsr                   Show Bootstrap Router information.
```

```
 interface              Show PIM interface information.
 mroute                 Show PIM-specific information from the IP multicast routing table.
 neighbor               Show PIM neighbor information.
 pending                Show (*,G) and (S,G) Join Pending Information.
 rp-candidate           Show Candidate-RP operational and configuration information.
 rp-set                 Show RP-Set information available on the router.
 rpf-override           Show the PIM RPF override entries.
 <cr>


ArubaOS-Switch# show ip mroute
 interface              Show IP multicast routing interfaces' information.
 IP-ADDR                Show detailed information for the specified entry from the IP
                        multicast routing table.
 <cr>
```

Comware5

```
[Comware5]multicast routing-enable


[Comware5]interface Vlan-interface 220

[Comware5-Vlan-interface220]pim ?
  bfd                     Enable BFD for PIM on interface
  bsr-boundary            Bootstrap router boundary
  dm                      Enable PIM dense mode
  hello-option            Specify hello option
  holdtime                Specify holdtime
  ipv6                    PIM IPv6 status and configuration information
  neighbor-policy         Policy to accept PIM hello messages
  require-genid           Require generation id
  sm                      Enable PIM sparse/SSM mode
  state-refresh-capable   State-refresh capability
  timer                   Specify PIM timer
  triggered-hello-delay   Triggered hello delay

[Comware5-Vlan-interface220]pim sm ?
  <cr>

[Comware5-Vlan-interface220]pim sm


[Comware5-Vlan-interface220]pim

[Comware5-pim]?
Pim protocol view commands:
  auto-rp                       Auto rendezvous point
  bidir-pim                     Specify parameters for bidirectional PIM
  bsm-fragment                  Semantic fragmentation of bootstrap messages
  bsr-policy                    Policy to accept PIM BSR messages
  c-bsr                         Candidate bootstrap router
  c-rp                          Candidate rendezvous point
  cfd                           Connectivity fault detection (IEEE 802.1ag)
  crp-policy                    Policy to accept PIM CRP messages
  display                       Display current system information
  dscp                          Differentiated Services Codepoint (DSCP)
  hello-option                  Specify hello option
  holdtime                      Specify holdtime
  jp-pkt-size                   Maximum join/prune packet size
  jp-queue-size                 Maximum join/prune entries sent once
  mtracert                      Trace route to multicast source
  ping                          Ping function
  probe-interval                Probe interval
```

```
  prune                          Prune delay
  quit                           Exit from current command view
  register-policy                Register policy
  register-suppression-timeout   Register suppress time
  register-whole-checksum        Checksum the whole of register packet
  return                         Exit to User View
  save                           Save current configuration
  source-lifetime                Source lifetime
  source-policy                  Source policy
  spt-switch-threshold           Data speed threshold for switchover to the SPT
  ssm-policy                     SSM policy
  state-refresh-interval         State refresh interval
  state-refresh-rate-limit       State refresh rate limit
  state-refresh-ttl              TTL of PIM DM state refresh message
  static-rp                      Static rendezvous point
  timer                          Specify PIM timer
  tracert                        Trace route function
  undo                           Cancel current settings

[Comware5-pim]static-rp ?
  X.X.X.X  Static rendezvous point address

[Comware5-pim]static-rp 10.1.220.1 ?
  INTEGER<2000-2999>  Apply basic acl
  bidir               Bidirectional PIM
  preferred           Prefer to choose static RP if there are conflicts with
                      BSR and Auto-RP mechanisms
  <cr>

[Comware5-pim]static-rp 10.1.220.1

[Comware5-pim]c-rp ?
  LoopBack                LoopBack interface
  Vlan-interface          VLAN interface
  advertisement-interval  Candidate rendezvous point advertisement-interval
  holdtime                Candidate rendezvous point holdtime

[Comware5-pim]c-rp Vlan-interface 220 ?
  advertisement-interval  Candidate rendezvous point advertisement-interval
  bidir                   Bidirectional PIM
  group-policy            Candidate rendezvous point acl number
  holdtime                Candidate rendezvous point holdtime
  priority                Candidate rendezvous point priority
  <cr>

[Comware5-pim]c-rp Vlan-interface 220

[Comware5-pim]c-bsr ?
  LoopBack        LoopBack interface
  Vlan-interface  VLAN interface
  admin-scope     Administrative scope candidate bootstrap router
  global          Global scope candidate bootstrap router
  group           Candidate bootstrap router group
  hash-length     Mask length of the RP Hash function
  holdtime        Candidate bootstrap router holdtime
  interval        Candidate bootstrap router interval
  priority        Candidate bootstrap router priority

[Comware5-pim]c-bsr Vlan-interface ?
  <1,100,220,230,240>  VLAN interface

[Comware5-pim]c-bsr Vlan-interface 220 ?
  INTEGER<0-32>  Mask length of the RP Hash function
```

```
  <cr>

[Comware5-pim]c-bsr Vlan-interface 220


[Comware5]display pim ?
  all-instance     All vpn-instances
  bsr-info         Bootstrap router information
  claimed-route    PIM claim route information
  control-message  PIM control message information
  df-info          Designated forwarder information of bidirectional PIM
  grafts           PIM unacknowledged grafts' information
  interface        PIM-enabled interface
  ipv6             PIM IPv6 status and configuration information
  join-prune       PIM join prune queue
  neighbor         PIM neighbor information
  routing-table    PIM routing table
  rp-info          RP information
  vpn-instance     Specify vpn-instance


[Comware5]display multicast routing-table ?
  X.X.X.X             Group address
  X.X.X.X             Source address
  all-instance        All vpn-instances
  incoming-interface  Incoming interface
  outgoing-interface  Outgoing interface
  static              Static configuration
  vpn-instance        VPN instance
  |                   Matching output
  <cr>
```

Comware7

```
[Comware7]multicast routing


[Comware7]interface Vlan-interface 220

[Comware7-Vlan-interface220]pim ?
  bfd                    Enable BFD for PIM
  bsr-boundary           Specify Bootstrap Router (BSR) message boundary
  dm                     Enable Dense Mode (DM)
  hello-option           Specify hello option
  holdtime               Specify holdtime timer
  neighbor-policy        Specify a legal source address range for hello messages
  passive                Enable passive capability
  require-genid          Require generation ID in hello messages
  sm                     Enable Sparse Mode (SM)
  state-refresh-capable  Enable state refresh capability
  timer                  Specify a timer
  triggered-hello-delay  Specify the maximum delay between two hello messages

[Comware7-Vlan-interface220]pim sm ?
  <cr>

[Comware7-Vlan-interface220]pim sm


[Comware7-Vlan-interface220]pim

[Comware7-pim]?
Pim protocol view commands:
  auto-rp                   Configure auto-RP
```

```
  bidir-pim                  Configure Bidirectional PIM
  bidir-rp-limit             Specify the maximum number of BIDIR-PIM RPs
  bsm-fragment               Bootstrap Message (BSM) semantic fragmentation
  bsr-policy                 Specify a legal Bootstrap Router (BSR) address range
  c-bsr                      Specify Candidate-BSR (C-BSR)
  c-rp                       Specify Candidate-RP (C-RP)
  cfd                        Connectivity Fault Detection (CFD) module
  crp-policy                 Specify a legal C-RP address range and the served
                             multicast group range
  diagnostic-logfile         Diagnostic log file configuration
  display                    Display current system information
  hello-option               Specify hello option
  holdtime                   Specify holdtime timer
  jp-pkt-size                Specify the maximum size of each join/prune message
  logfile                    Log file configuration
  monitor                    System monitor
  ping                       Ping function
  quit                       Exit from current command view
  register-policy            Register policy
  register-whole-checksum    Calculate the checksum based on an entire register
                             message
  return                     Exit to User View
  save                       Save current configuration
  security-logfile           Security log file configuration
  source-lifetime            Specify a source lifetime
  source-policy              Specify a multicast data filter
  spt-switch-threshold       Specify a traffic rate threshold for triggering a
                             switchover to SPT
  ssm-policy                 SSM policy
  state-refresh-interval     Specify a interval between state refresh messages
  state-refresh-rate-limit   Specify a time that the device waits for a new state
                             refresh message
  state-refresh-ttl          Specify a TTL value for state refresh messages
  static-rp                  Specify static RP
  timer                      Specify a timer
  tracert                    Tracert function
  undo                       Cancel current setting

[Comware7-pim]static-rp ?
  X.X.X.X  Static RP address

[Comware7-pim]static-rp 10.1.220.1 ?
  INTEGER<2000-2999>  Specify a basic ACL
  bidir               Specify the static RP to serve BIDIR-PIM
  preferred           Give priority to the static RP if the static RP conflicts
                      with the dynamic RP
  <cr>

[Comware7-pim]static-rp 10.1.220.1

[Comware7-pim]c-rp ?
  X.X.X.X  IP address

[Comware7-pim]c-rp 10.1.220.1 ?
  advertisement-interval  Specify an interval between two C-RP advertisement
                          messages
  bidir                   Specify the C-RP to serve BIDIR-PIM
  group-policy            Specify a group policy
  holdtime                Specify a holdtime for the C-RP
  priority                Specify a priority for the C-RP
  <cr>

[Comware7-pim]c-rp 10.1.220.1
```

```
[Comware7-pim]c-bsr ?
  X.X.X.X  IP address

[Comware7-pim]c-bsr 10.1.220.1 ?
  hash-length  Specify a hash mask length
  priority     Specify a priority for the C-BSR
  scope        Specify an admin-scope zone
  <cr>

[Comware7-pim]c-bsr 10.1.220.1


[Comware7]display pim ?
  bsr-info       Display Bootstrap Router (BSR) information
  c-rp           Display Candidate-RP (C-RP) information
  claimed-route  Display information about all routes that PIM uses
  df-info        Display Designated Forwarder (DF) information
  interface      Display PIM information on an interface
  neighbor       Display PIM neighbor information
  routing-table  Display PIM routing table information
  rp-info        Display Rendezvous Point (RP) information
  statistics     Display PIM packet statistics information
  vpn-instance   Specify a VPN instance


[Comware7]display multicast routing-table ?
  >                   Redirect it to a file
  >>                  Redirect it to a file in append mode
  X.X.X.X             Group address
  X.X.X.X             Source address
  incoming-interface  Specify incoming interface in entries
  outgoing-interface  Specify outgoing interface in entries
  static              Static information
  |                   Matching output
  <cr>
```

Cisco

```
Cisco(config)#ip multicast-routing distributed


Cisco(config)#interface vlan 220

Cisco(config-if)#ip pim ?
  bidir-neighbor-filter  PIM bidir capable peering filter
  bsr-border             Border of PIM domain
  dense-mode             Enable PIM dense-mode operation
  dr-priority            PIM router DR priority
  nbma-mode              Use Non-Broadcast Multi-Access (NBMA) mode on
                         interface
  neighbor-filter        PIM peering filter
  passive                Enable PIM passive interface operation
  query-interval         PIM router query interval
  sparse-dense-mode      Enable PIM sparse-dense-mode operation
  sparse-mode            Enable PIM sparse-mode operation
  state-refresh          PIM DM State-Refresh configuration

Cisco(config-if)#ip pim sparse-mode

Cisco(config-if)#exit


Cisco(config)#ip pim ?
```

```
  accept-register       Registers accept filter
  accept-rp             RP accept filter
  autorp                Configure AutoRP global operations
  bidir-enable          Enable Bidir-PIM
  bidir-offer-interval  DF election offer message interval
  bidir-offer-limit     number of unanswered offers before becoming DF
  bsr-candidate         Candidate bootstrap router (candidate BSR)
  dm-fallback           Fallback group mode is Dense
  log-neighbor-changes  Log PIM neighbor up/down and DR changes
  register-rate-limit   Rate limit for PIM data registers
  register-source       Source address for PIM Register
  rp-address            PIM RP-address (Rendezvous Point)
  rp-announce-filter    Auto-RP announce message filter
  rp-candidate          To be a PIMv2 RP candidate
  send-rp-announce      Auto-RP send RP announcement
  send-rp-discovery     Auto-RP send RP discovery message (as RP-mapping agent)
  sparse                This command is specific to PIM-Sparse Mode
  spt-threshold         Source-tree switching threshold
  ssm                   Configure Source Specific Multicast
  state-refresh         PIM DM State-Refresh configuration
  v1-rp-reachability    Send PIMv1 RP-reachability packet
  vrf                   Select VPN Routing/Forwarding instance

Cisco(config)#ip pim rp-address ?
  A.B.C.D  IP address of Rendezvous-point for group

Cisco(config)#ip pim rp-address 10.1.220.1 ?
  <1-99>       Access-list reference for group
  <1300-1999>  Access-list reference for group (expanded range)
  WORD         IP Named Standard Access list
  override     Overrides dynamically learnt RP mappings
  <cr>

Cisco(config)#ip pim rp-address 10.1.220.1

Cisco(config)#ip pim rp-candidate ?
  Async               Async interface
  Auto-Template       Auto-Template interface
  BVI                 Bridge-Group Virtual Interface
  CTunnel             CTunnel interface
  Dialer              Dialer interface
  FastEthernet        FastEthernet IEEE 802.3
  Filter              Filter interface
  Filtergroup         Filter Group interface
  GigabitEthernet     GigabitEthernet IEEE 802.3z
  GroupVI             Group Virtual interface
  Lex                 Lex interface
  Loopback            Loopback interface
  Null                Null interface
  Port-channel        Ethernet Channel of interfaces
  Portgroup           Portgroup interface
  Pos-channel         POS Channel of interfaces
  TenGigabitEthernet  Ten Gigabit Ethernet
  Tunnel              Tunnel interface
  Vif                 PGM Multicast Host interface
  Virtual-Template    Virtual Template interface
  Virtual-TokenRing   Virtual TokenRing
  Vlan                Catalyst Vlans
  fcpa                Fiber Channel

Cisco(config)#ip pim rp-candidate vlan ?
  <1-4094>  Vlan interface number
```

```
Cisco(config)#ip pim rp-candidate vlan 220 ?
  group-list  group-list
  interval    RP candidate advertisement interval
  priority    RP candidate priority
  <cr>

Cisco(config)#ip pim rp-candidate vlan 220

Cisco(config)#ip pim bsr-candidate ?
  Async               Async interface
  Auto-Template       Auto-Template interface
  BVI                 Bridge-Group Virtual Interface
  CTunnel             CTunnel interface
  Dialer              Dialer interface
  FastEthernet        FastEthernet IEEE 802.3
  Filter              Filter interface
  Filtergroup         Filter Group interface
  GigabitEthernet     GigabitEthernet IEEE 802.3z
  GroupVI             Group Virtual interface
  Lex                 Lex interface
  Loopback            Loopback interface
  Null                Null interface
  Port-channel        Ethernet Channel of interfaces
  Portgroup           Portgroup interface
  Pos-channel         POS Channel of interfaces
  TenGigabitEthernet  Ten Gigabit Ethernet
  Tunnel              Tunnel interface
  Vif                 PGM Multicast Host interface
  Virtual-Template    Virtual Template interface
  Virtual-TokenRing   Virtual TokenRing
  Vlan                Catalyst Vlans
  fcpa                Fiber Channel

Cisco(config)#ip pim bsr-candidate vlan ?
  <1-4094>  Vlan interface number

Cisco(config)#ip pim bsr-candidate vlan 220 ?
  <0-32>  Hash Mask length for RP selection
  <cr>

Cisco(config)#ip pim bsr-candidate vlan 220


Cisco#show ip pim ?
  autorp      Global AutoRP information
  boundary    debug boundary comand
  bsr-router  Bootstrap router (v2)
  interface   PIM interface information
  mdt         Multicast tunnel information
  neighbor    PIM neighbor information
  rp          PIM Rendezvous Point (RP) information
  rp-hash     RP to be chosen based on group selected
  vrf         Select VPN Routing/Forwarding instance


Cisco#show ip mroute ?
  Hostname or A.B.C.D  Source or group IP name or address
  active               Active multicast sources
  bidirectional        Show bidirectional multicast routes
  count                Route and packet count data
  dense                Show dense multicast routes
  interface            Interface information
  proxy                List proxies
```

```
  pruned                Pruned routes
  sparse                Show sparse multicast routes
  ssm                   show SSM multicast routes
  static                Static multicast routes
  summary               Provide abbreviated display
  verbose               Verbose
  vrf                   Select VPN Routing/Forwarding instance
  |                     Output modifiers
  <cr>
```

c) IGMP

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(vlan-220)# ip igmp	[Comware-Vlan-interface220]igmp enable	Enabling PIM on an interface also enables IGMP operation on that interface.
ArubaOS-Switch(vlan-220)#Igmp reload		Cisco(config)# ip igmp snooping
ArubaOS-Switch(vlan-220)#Mld reload		Cisco(config-vlan)#ipv6 mld version value
ArubaOS-Switch(vlan-220)#ip igmp lookup-mode <ip/mac>		Cisco(config-vlan)#ip igmp snooping explicit-tracking
ArubaOS-Switch(vlan-220)#ip igmp version 3		
ArubaOS-Switch(vlan-220)#show ip igmp vlan <vid> group <tab key/?>		Cisco(config-vlan)#show ip igmp snooping [[vlan] vlan-id]
ArubaOS-Switch(vlan-220)#show ip igmp vlan <vid> group <ip4-addr> <tab key/?>		Cisco(config-vlan)# show ip igmp snooping groups [[vlan] vlan-id] detail
ArubaOS-Switch(vlan-220)#show ip igmp vlan 1 group port <tab key/?>		Cisco(config-vlan)# show ip igmp snooping querier [[vlan] vlan-id]
ArubaOS-Switch(vlan-220)#Show ip igmp vlan 2 groups		Cisco(config-vlan)# show ip igmp snooping explicit tracking [[vlan] vlan-id]

ArubaOS-Switch

```
ArubaOS-Switch(vlan-200)# ip igmp
 auto                   Instruct the device to monitor incoming multicast traffic on the
                        specified ports (this is the default behavior).
 blocked                Instruct the device to drop incoming multicast packets received on
                        the specified ports.
 fastleave              Enables or disables IGMP Fast Leaves.
 forcedfastleave        When enabled, this feature forces IGMP Fast Leaves to occur even
                        when the port is cascaded.
 forward                Instruct the device to forward incoming multicast packets received
                        on the specified ports.
 querier                Specify querier/non-querier capability for the VLAN.
 static-group           Creates the igmp static group with the specified IP address.
 <cr>

ArubaOS-Switch(vlan-220)# ip igmp
```

Comware5

```
[Comware5-Vlan-interface220]igmp ?
  enable                      Enable group membership protocol
  group-limit                 Configure group limit on this interface
  group-policy                Specify group policy
  host-tracking               Configure host-tracking
  last-member-query-interval  Specify last member query interval
  max-response-time           Specify maximum response time
  proxying                    Specify parameters for Proxying
```

```
  require-router-alert        Specify required router alert
  robust-count                Specify robustness count
  send-router-alert           Specify send router alert
  ssm-mapping                 Specify parameters for SSM mapping
  startup-query-count         Specify startup query count
  startup-query-interval      Specify startup query interval
  static-group                Specify static group
  timer                       Specify timer
  version                     Specify version

[Comware5-Vlan-interface220]igmp enable ?
  <cr>

[Comware5-Vlan-interface220]igmp enable
```

Comware7

```
[Comware7-Vlan-interface220]igmp ?
  enable                          Enable Internet group management protocol
  fast-leave                      Leave groups without sending last member query
  group-policy                    Specify group policy to accept IGMP joins
  host                            Specify IGMP host
  last-member-query-count         Specify a last member query count
  last-member-query-interval      Specify a last member query interval
  max-response-time               Specify a maximum response time
  other-querier-present-interval  Specify an other querier present interval
  query-interval                  Specify a general query interval
  robust-count                    Specify a robustness count
  startup-query-count             Specify a startup query count
  startup-query-interval          Specify a startup query interval
  static-group                    Specify a static group
  version                         Specify a version

[Comware7-Vlan-interface220]igmp enable ?
  <cr>

[Comware7-Vlan-interface220]igmp enable
```

Cisco

Enabling PIM on an interface also enables IGMP operation on that interface.

Chapter 31 Spanning Tree Hardening

This chapter compares the commands you use to configure:

- Unidirectional Link Detection (UDLD) and Device Link Detection Protocol (DLDP)
- Bridge Protocol Data Unit (BPDU) protection and BPDU guard
- Loop protection
- Root guard

UDLD monitors a link between two switches and blocks the ports on both ends of the link if the link fails at any point between the two devices. This feature is particularly useful for detecting failures in fiber links and trunks.

DLDP is a technology for dealing with unidirectional links (fiber links or copper twisted-pair links) that may occur in a network. On detecting a unidirectional link, DLDP, as configured, can shut down the related port automatically or prompt users to take actions to avoid network problems.

BPDU protection is a security feature designed to protect the active STP topology by preventing spoofed BPDU packets from entering the STP domain. In a typical implementation, you would apply BPDU protection to edge ports connected to end user devices that do not run STP. If STP BPDU packets are received on a protected port, the feature will disable that port and alert the network manager via an SNMP trap.

In cases where you cannot use spanning tree to prevent loops at the edge of the network, loop protection may provide a suitable alternative. Loop protection operates in two modes:

- *Untagged* is the default mode. You can use this mode to find loops in untagged downlinks.
- *Tagged VLAN* finds loops on tagged VLANs. You can use this mode to detect loops in tagged-only uplinks where you cannot enable STP.

The cases where loop protection might be chosen ahead of spanning tree to detect and prevent loops are as follows:

- On ports with client authentication, when spanning tree is enabled on a switch that use 802.1X, Web authentication, and MAC authentication, loops may go undetected. For example, spanning tree packets that are looped back to an edge port will not be processed because they have a different broadcast/multicast MAC address from the client-authenticated MAC address. To ensure that client-authenticated edge ports get blocked when loops occur, you should enable loop protection on those ports.

- On ports connected to unmanaged devices, spanning tree cannot detect the formation of loops where there is an unmanaged device on the network that does not process spanning tree packets and simply drops them. Loop protection has no such limitation; you can use it to prevent loops on unmanaged switches.

By keeping receiving BPDUs from the upstream device, a device can maintain the state of the root port and blocked ports. However, because of link congestion or unidirectional link failures, these ports may fail to receive BPDUs from the upstream devices. The device will reselect the port roles: Those ports in forwarding state that failed to receive upstream BPDUs will become designated ports, and the blocked ports will transition to the forwarding state, resulting in loops in the switched network. The loop guard function can suppress the occurrence of such loops.

The initial state of a loop-guard-enabled port is discarding in every Multiple Spanning Tree Instance (MSTI). When the port receives BPDUs, its state transitions normally; otherwise, it stays in the discarding state to prevent temporary loops.

When a port is enabled as root-guard, it cannot be selected as the root port even if it receives superior STP BPDUs. The port is assigned an "alternate" port role and enters a blocking state if it receives superior STP BPDUs.

A superior BPDU contains "better" information on the root bridge and path cost to the root bridge, which would normally replace the current root bridge selection.

The superior BPDUs that a port enabled as root-guard receives are ignored. All other BPDUs are accepted, and the external devices may belong to the spanning tree as long as they do not claim to be the Root device.

Use this command on MSTP switch ports that are connected to devices located in other administrative network domains to:

- Ensure the stability of the core MSTP network topology so that undesired or damaging influences external to the network do not enter
- Protect the configuration of the Common and Internal Spanning Tree (CIST) root bridge that serves as the common root for the entire network

a) UDLD and DLDP

ArubaOS-Switch	Comware5	Cisco
	[Comware5]dldp enable	
ArubaOS-Switch(config)# interface 17	[Comware5]interface g1/0/17	Cisco(config)#interface g1/0/17
ArubaOS-Switch(eth-17)# link-keepalive	[Comware5-GigabitEthernet1/0/17]dldp enable	Cisco(config-if)#udld port
ArubaOS-Switch# show link-keepalive	[Comware5]display dldp	Cisco#show udld g1/0/17
ArubaOS-Switch# show link-keepalive statistics	[Comware5]display dldp statistics	
	Comware7	
	[Comware7] dldp global enable	
	[Comware7]interface g1/0/17	
	[Comware7-GigabitEthernet1/0/17]dldp enable	
	[Comware7]display dldp	
	[Comware7]display dldp statistics	

ArubaOS-Switch

```
ArubaOS-Switch(config)# interface 17

ArubaOS-Switch(eth-17)# link-keepalive ?
 vlan                   Set vlan-id for tagged UDLD control packets.
 <cr>

ArubaOS-Switch(eth-17)# link-keepalive


ArubaOS-Switch# show link-keepalive ?
statistics             Show detailed statistics for all link-keepalive enabled ports.
 <cr>


ArubaOS-Switch# show link-keepalive

 Status and Configuration - UniDirectional Link Detection (UDLD)

  Keepalive Retries   : 4
  Keepalive Interval  : 5000 ms
  Keepalive Mode      : forward-then-verify

                 Physical          Keepalive Adjacent      UDLD
  Port  Enabled  Status            Status    Switch        VLAN
  ----- -------- ---------------- --------- ------------- ----------
  17    Yes      up                failure   000000-000000 untagged

ArubaOS-Switch# show link-keepalive statistics

 Status and Counters - UniDirectional Link Detection (UDLD)

  Port                : 17
```

```
  Current State      : failure          Neighbor MAC Addr  : 000000-000000
  UDLD Pkts Sent     : 113              Neighbor Port      : 0
  UDLD Pkts Received : 0                State Transitions  : 1
  Port Blocking      : Yes              Link-VLAN          : untagged
```

Comware5

```
[Comware5]dldp ?
  authentication-mode      Specify password and authentication mode of DLDP
                           packet
  delaydown-timer          Specify the value of delaydown timer
  enable                   DLDP enable
  interval                 Specify the value of advertisement packet timer
  reset                    DLDP reset
  unidirectional-shutdown  Specify the mode of DLDP unidirectional shutdown
  work-mode                Set the work mode of DLDP

[Comware5]dldp enable


[Comware5]interface g1/0/17

[Comware5-GigabitEthernet1/0/17]dldp ?
  enable  DLDP enable
  reset   DLDP reset

[Comware5-GigabitEthernet1/0/17]dldp enable


[Comware5]display dldp ?
  GigabitEthernet  GigabitEthernet interface
  statistics       DLDP Packet Statistics
  |                Matching output
  <cr>

[Comware5]display dldp
DLDP global status : enable
 DLDP interval : 5s
 DLDP work-mode : normal
 DLDP authentication-mode : none
 DLDP unidirectional-shutdown : auto
 DLDP delaydown-timer : 1s
 The number of enabled ports is 1.

Interface GigabitEthernet1/0/17
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 0.

[Comware5]display dldp statistics
Interface GigabitEthernet1/0/17
 Packets sent : 107
 Packets received : 0
 Invalid packets received : 0
 Loop packets received : 0
 Authentication failed packets received : 0
 Valid packets received : 0
```

Comware7

```
[Comware7]dldp ?
  authentication-mode      Set the authentication mode for DLDP packets
  authentication-password  Set the password for DLDP packets
  delaydown-timer          Set the delaydown timer
  global                   Specify global DLDP
  interval                 Set the interval of sending advertisement packets
```

```
  unidirectional-shutdown  Specify the port shutdown mode upon detecting a
                           unidirectional link

[Comware7]dldp global ?
  enable  Enable DLDP

[Comware7]dldp global enable ?
  <cr>

[Comware7]dldp global enable


[Comware7]interface g1/0/17

[Comware7-GigabitEthernet1/0/17]dldp ?
  enable  Enable DLDP

[Comware7-GigabitEthernet1/0/17]dldp enable


[Comware7]display dldp ?
  >           Redirect it to a file
  >>          Redirect it to a file in append mode
  interface   Specify an interface
  statistics  DLDP packet statistics
  |           Matching output
  <cr>

[Comware7]display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: None
 DLDP unidirectional-shutdown mode: Auto
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 1

Interface GigabitEthernet1/0/17
 DLDP port state: Unidirectional
 Number of the port's neighbors: 0

[Comware7]display dldp statistics
Interface GigabitEthernet1/0/17
 Packets sent: 66
 Packets received: 0
 Invalid packets received: 0
 Loopback packets received: 0
 Authentication-failed packets received: 0
 Valid packets received: 0
```

Cisco

```
Cisco(config)#interface g1/0/17

Cisco(config-if)#udld ?
  port  Enable UDLD protocol on this interface

Cisco(config-if)#udld port ?
  aggressive  Enable UDLD protocol in aggressive mode on this interface
  <cr>

Cisco(config-if)#udld port


Cisco#show udld ?
```

```
  Async                Async interface
  Auto-Template        Auto-Template interface
  BVI                  Bridge-Group Virtual Interface
  CTunnel              CTunnel interface
  Dialer               Dialer interface
  FastEthernet         FastEthernet IEEE 802.3
  Filter               Filter interface
  Filtergroup          Filter Group interface
  GigabitEthernet      GigabitEthernet IEEE 802.3z
  Group-Async          Async Group interface
  GroupVI              Group Virtual interface
  Lex                  Lex interface
  Loopback             Loopback interface
  Null                 Null interface
  Port-channel         Ethernet Channel of interfaces
  Portgroup            Portgroup interface
  Pos-channel          POS Channel of interfaces
  TenGigabitEthernet   Ten Gigabit Ethernet
  Tunnel               Tunnel interface
  Vif                  PGM Multicast Host interface
  Virtual-Template     Virtual Template interface
  Virtual-TokenRing    Virtual TokenRing
  Vlan                 Catalyst Vlans
  fcpa                 Fiber Channel
  neighbors            UDLD Neighbors Summary
  |                    Output modifiers
  <cr>

Cisco#show udld g1/0/17

Interface Gi1/0/17
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Advertisement
Message interval: 7
Time out interval: 5
No neighbor cache information stored
```

b) BPDU Protection and BPDU Guard

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# spanning-tree bpdu-protection-timeout 300		Cisco(config)#interface g1/0/17
ArubaOS-Switch(config)# spanning-tree 17 bpdu-protection		Cisco(config-if)#spanning-tree bpduguard enable
ArubaOS-Switch(config)# spanning-tree 17 bpdu-filter		Cisco(config-if)#spanning-tree bpdufilter enable
	[Comware]stp bpdu-protection	

ArubaOS-Switch

```
ArubaOS-Switch(config)# spanning-tree bpdu-protection-timeout 300


ArubaOS-Switch(config)# spanning-tree 17 bpdu-protection


ArubaOS-Switch(config)# spanning-tree 17 bpdu-filter
The BPDU filter allows the port to go into a continuous
forwarding mode and spanning tree will not interfere, even if
the port would cause a loop to form in the network topology.
If you suddenly experience high traffic load, disable the port
and reconfigure the BPDU filter with the CLI command(s):
"no spanning tree PORT_LIST bpdu-filter"
"no spanning tree PORT_LIST pvst-filter"
```

Comware

Make this configuration on a device with edge ports configured.

```
[Comware]stp bpdu-protection
```

Cisco

```
Cisco(config)#interface g1/0/17

Cisco(config-if)#spanning-tree bpduguard enable
```

(Note: the port must manually put back in service if this feature is triggered)

```
Cisco(config-if)#spanning-tree bpdufilter enable
```

c) Loop Protection

ArubaOS-Switch	Comware5	Cisco
	[Comware5]loopback-detection enable	
ArubaOS-Switch(config)# loop-protect 17 receiver-action send-disable	[Comware5]interface g1/0/17 [Comware5-GigabitEthernet1/0/17] loopback-detection enable [Comware5-GigabitEthernet1/0/17] loopback-detection action shutdown	Cisco(config)#interface g1/0/17 Cisco(config-if)#spanning-tree guard loop
	Comware7	
	[Comware7]loopback-detection global enable vlan 1	
	[Comware7]interface g1/0/17 [Comware7-GigabitEthernet1/0/17] loopback-detection enable vlan 1 [Comware7-GigabitEthernet1/0/17] loopback-detection action shutdown	

ArubaOS-Switch

```
ArubaOS-Switch(config)# loop-protect 17 receiver-action send-disable
```

Comware5

```
[Comware5]loopback-detection enable


[Comware5]interface g1/0/17

[Comware5-GigabitEthernet1/0/17]loopback-detection ?
  action     Set action mode for the interface involved in loopback
  control    Set port loopback detection control
  enable     Enable port loopback detection
  per-vlan   Port loopback detection per vlan

[Comware5-GigabitEthernet1/0/17]loopback-detection enable

[Comware5-GigabitEthernet1/0/17]loopback-detection action shutdown
```

Comware7

```
[Comware7]loopback-detection ?
  global          Specify loopback detection globally
  interval-time   Set loopback detection interval

[Comware7]loopback-detection global ?
  action  Set the action mode for interfaces involved in loopback
  enable  Enable loopback detection

[Comware7]loopback-detection global enable ?
```

```
  vlan  Specify a VLAN list

[Comware7]loopback-detection global enable vlan ?
  INTEGER<1-4094>  VLAN ID
  all              Specify all VLANs

[Comware7]loopback-detection global enable vlan 1 ?
  INTEGER<1-4094>  VLAN ID
  to               Specify the end VLAN ID of a VLAN range
  <cr>

[Comware7]loopback-detection global enable vlan 1


[Comware7]interface g1/0/17

[Comware7-GigabitEthernet1/0/17]loopback-detection ?
  action  Set the action mode for interfaces involved in loopback
  enable  Enable loopback detection

[Comware7-GigabitEthernet1/0/17]loopback-detection enable ?
  vlan  Specify a VLAN list

[Comware7-GigabitEthernet1/0/17]loopback-detection enable vlan 1 ?
  INTEGER<1-4094>  VLAN ID
  to               Specify the end VLAN ID of a VLAN range
  <cr>

[Comware7-GigabitEthernet1/0/17]loopback-detection enable vlan 1

[Comware7-GigabitEthernet1/0/17]loopback-detection action ?
  block        Block mode
  no-learning  No-learning mode
  shutdown     Shutdown mode

[Comware7-GigabitEthernet1/0/17]loopback-detection action shutdown ?
  <cr>

[Comware7-GigabitEthernet1/0/17]loopback-detection action shutdown
```

Cisco

```
Cisco(config)#interface g1/0/17

Cisco(config-if)#spanning-tree guard loop
```

d) Root Guard

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# spanning-tree 17 root-guard	[Comware]interface g1/0/17 [Comware-GigabitEthernet1/0/17]stp root-protection	Cisco(config)#interface g1/0/17 Cisco(config-if)#spanning-tree guard root
ArubaOS-Switch(config)# spanning-tree 17 tcn-guard		

ArubaOS-Switch
ArubaOS-Switch(config)# spanning-tree 17 root-guard ArubaOS-Switch(config)# spanning-tree 17 tcn-guard
Comware
[Comware]interface g1/0/17 [Comware-GigabitEthernet1/0/17]stp root-protection
Cisco
Cisco(config)#interface g1/0/17 Cisco(config-if)#spanning-tree guard root

Chapter 32 DHCP Snooping

This chapter compares commands you can use to enable protections for Dynamic Host Configuration Protocol (DHCP), thereby preventing malicious users from using DHCP to gather information about the network or attack it.

You can use DHCP snooping to help avoid the Denial of Service attacks that result from unauthorized users adding a DHCP server to the network that then providing invalid configuration data to other DHCP clients on the network. DHCP snooping enables you to distinguish between trusted ports connected to a DHCP server or switch and untrusted ports connected to end users. DHCP packets are forwarded between trusted ports without inspection. DHCP packets received on other switch ports are inspected before being forwarded. Packets from untrusted sources are dropped.

ArubaOS-Switch	Comware5	Cisco
ArubaOS-Switch(config)# dhcp-snooping	[Comware5]dhcp-snooping	Cisco(config)#ip dhcp snooping
ArubaOS-Switch(config)# dhcp-snooping authorized-server 10.0.100.251		
ArubaOS-Switch(config)# dhcp-snooping database file tftp://10.0.100.111/ArubaOS-Switch_dhcp.txt		Cisco(config)#ip dhcp snooping database tftp://10.0.100.111/Cisco_dhcp.txt
	[Comware5]dhcp-snooping binding database filename Comware5_dhcp.txt	
ArubaOS-Switch(config)# dhcp-snooping vlan 220		Cisco(config)#ip dhcp snooping vlan 220
ArubaOS-Switch(config)# dhcp-snooping trust 1	[Comware5]interface g1/0/6 [Comware5-GigabitEthernet1/0/6]dhcp-snooping trust	Cisco(config)#interface g1/0/6 Cisco(config-if)#ip dhcp snooping trust
ArubaOS-Switch# show dhcp-snooping	[Comware5]display dhcp-snooping [Comware5]display dhcp-snooping trust	Cisco#show ip dhcp snooping
	[Comware5]display dhcp-snooping binding database	Cisco#show ip dhcp snooping database
ArubaOS-Switch# show dhcp-snooping stats	[Comware5]display dhcp-snooping packet statistics	Cisco#show ip dhcp snooping statistics detail
ArubaOS-Switch(config)#clear dhcp-snooping binding all		Cisco(config)#clear ip dhcp snoop bind
ArubaOS-Switch(config)#clear dhcp-snooping binding ip <IP-ADDR>		Cisco(config)#clear ip dhcp snooping track host

ArubaOS-Switch(config)#clear dhcp-snooping binding port <PORT NUM>		Cisco(config)#clear ip dhcp snooping track hosts statistics
ArubaOS-Switch(config)#clear dhcp-snooping binding vlan <VLAN ID>		Cisco(config)#clear ip dhcp snooping database statistics
	Comware7	
	[Comware7]dhcp snooping enable	
	[Comware7]dhcp snooping binding database filename url tftp://10.0.100.111/Comware7_dhcp.txt	
	[Comware7]interface g1/0/6 [Comware7-GigabitEthernet1/0/6]dhcp snooping trust	
	[Comware7]interface g1/0/4 [Comware7-GigabitEthernet1/0/4]dhcp snooping binding record	
	[Comware7]display dhcp snooping binding [Comware7]display dhcp snooping trust	
	[Comware7]display dhcp snooping binding database	
	[Comware7]display dhcp snooping packet statistics	

ArubaOS-Switch

```
ArubaOS-Switch(config)# dhcp-snooping ?
 authorized-server     Add an authorized DHCP server address.
 database              Configure lease database transfer options.
 max-bindings          Set the maximum number of DHCP bindings allowed.
 option                Configure option 82 processing of DHCP packets.
 trust                 Configure trusted interfaces for DHCP server packets.
 verify                Enable DHCP packet MAC address validation.
 vlan                  Enable DHCP snooping on one or more VLANs.
 <cr>

ArubaOS-Switch(config)# dhcp-snooping


ArubaOS-Switch(config)# dhcp-snooping authorized-server 10.0.100.251


ArubaOS-Switch(config)# dhcp-snooping database file tftp://10.0.100.111/ArubaOS-
Switch_dhcp.txt
```

```
ArubaOS-Switch(config)# dhcp-snooping option ?
 82                     Enable adding option 82 relay information to DHCP client packets
                        forwarded on trusted ports.

ArubaOS-Switch(config)# dhcp-snooping option 82 ?
 remote-id              Select the address used as the Remote ID.
 untrusted-policy       Policy for DHCP packets received on untrusted ports that contain
                        option 82.
 <cr>

ArubaOS-Switch(config)# dhcp-snooping option 82 remote-id ?
mac                    Use the switch MAC address as the ID (default)
 subnet-ip              Use the IP address of the client's VLAN (if set) as the ID.
 mgmt-ip                Use the management VLAN IP address (if set) as the ID.

ArubaOS-Switch(config)# dhcp-snooping option 82 untrusted-policy ?
 drop                   Drop packets (default)
 keep                   Forward packets unchanged
 replace                Replace option 82 information and forward


ArubaOS-Switch(config)# dhcp-snooping vlan 220


ArubaOS-Switch(config)# dhcp-snooping trust 1


ArubaOS-Switch# show dhcp-snooping ?
 binding                Show DHCP snooping binding information.
 stats                  Show DHCP snooping statistics.
 <cr>

ArubaOS-Switch# show dhcp-snooping

 DHCP Snooping Information

  DHCP Snooping              : Yes
  Enabled VLANs              : 220
  Verify MAC address         : Yes
  Option 82 untrusted policy : drop
  Option 82 insertion        : Yes
  Option 82 remote-id        : mac
  Store lease database       : Yes
  URL            : tftp://10.0.100.111/ArubaOS-Switch_dhcp.txt
  Read at boot   : no
  Write delay    : 300
  Write timeout  : 300
  File status    : up-to-date
  Write attempts : 1
  Write failures : 0
  Last successful file update : Sun May 17 16:40:54 2015


  Authorized Servers
  ------------------
  10.0.100.251


                  Max     Current Bindings
   Port  Trust  Bindings  Static   Dynamic
  -----  -----  --------  ----------------
```

```
    1     Yes      -        -        -
    4     No       -        -        1

  Ports 2-3,5-18,25-26,Trk1-Trk3 are untrusted


ArubaOS-Switch# show dhcp-snooping stats


Packet type  Action   Reason                        Count
 -----------  -------  ----------------------------  ---------
 server       forward  from trusted port              1
 client       forward  to trusted port                1
 server       drop     received on untrusted port     0
 server       drop     unauthorized server            0
 client       drop     destination on untrusted port  0
 client       drop     untrusted option 82 field      0
 client       drop     bad DHCP release request       0
 client       drop     failed verify MAC check        0
 client       drop     failed on max-binding limit    0
```

Comware5

```
[Comware5]dhcp-snooping ?
  binding  Specify DHCP Snooping bindings
  check    Check the DHCP packet
  <cr>

[Comware5]dhcp-snooping


[Comware5]dhcp-snooping binding database filename Comware5_dhcp.txt


[Comware5]interface g1/0/6

[Comware5-GigabitEthernet1/0/6]dhcp-snooping ?
  check            Check the DHCP packet
  information      Specify Option 82 service
  no-user-binding  Forbid DHCP Snooping learning
  rate-limit       Limit DHCP packet rate
  trust            Trusted port

[Comware5-GigabitEthernet1/0/6]dhcp-snooping trust ?
  <cr>

[Comware5-GigabitEthernet1/0/6]dhcp-snooping trust


[Comware5-GigabitEthernet1/0/6]dhcp-snooping information ?
  circuit-id  Specify the circuit ID
  enable      Enable Option 82
  format      Specify the mode of option 82
  remote-id   Specify the remote ID
  strategy    Specify the strategy to handle Option 82
  sub-option  Specify sub-options of Option 82
  vlan        Specify VLAN


[Comware5-GigabitEthernet1/0/6]dhcp-snooping information enable ?
  <cr>

[Comware5-GigabitEthernet1/0/6]dhcp-snooping information format ?
  normal    Normal mode
```

```
  private   Private mode
  standard  Standard mode
  verbose   Verbose mode

[Comware5-GigabitEthernet1/0/6]dhcp-snooping information remote-id ?
  format-type  Specify the format of remote ID
  string       Specify the content of remote ID

[Comware5-GigabitEthernet1/0/6]dhcp-snooping information strategy ?
  append   Append strategy
  drop     Drop strategy
  keep     Keep strategy
  replace  Replace strategy

[Comware5-GigabitEthernet1/0/6]dhcp-snooping information vlan ?
  INTEGER<1-4094>  VLAN ID

[Comware5-GigabitEthernet1/0/6]dhcp-snooping information vlan 220 ?
  circuit-id  Specify the circuit ID
  remote-id   Specify the remote ID
  sub-option  Specify sub-options of Option 82


[Comware5]display dhcp-snooping ?
  binding      Specify DHCP Snooping bindings
  information  Specify Option 82 service
  ip           Single client ip
  packet       Packet statistics function
  trust        Trusted port
  |            Matching output
  <cr>


[Comware5]display dhcp-snooping
 DHCP Snooping is enabled.
 The client binding table for all ports.
 Type : D--Dynamic , S--Static , R--Recovering
 Type IP Address      MAC Address    Lease        VLAN SVLAN Interface
 ==== =============== ============== ============ ==== ===== =================
 D    10.1.220.105    68b5-99d8-f726 86319        220  N/A   GE1/0/4
---   1 dhcp-snooping item(s) found   ---

[Comware5]display dhcp-snooping trust
 DHCP Snooping is enabled.
 DHCP Snooping trust becomes active.
 Interface                                       Trusted
 ========================                        ============
 GigabitEthernet1/0/6                            Trusted


[Comware5]display dhcp-snooping binding database
 File name               :   flash:/Comware5_dhcp.txt
 Update interval         :   Not configured
 Latest read time        :   -
 Latest write time       :   May 17 2015 16:45:03
 Status                  :   Last write succeeded.


[Comware5]display dhcp-snooping packet statistics
 DHCP packets received                   : 66
 DHCP packets sent                       : 4
 Packets dropped due to rate limitation : 0
 Dropped invalid packets                 : 0
```

Comware7

```
[Comware7]dhcp ?
  class     Create a DHCP class
  client    Configure a DHCP client
  dscp      Set the Differentiated Services Codepoint (DSCP) value
  enable    Enable DHCP
  relay     Configure a DHCP relay agent
  server    Configure a DHCP server
  snooping  Configure DHCP snooping

[Comware7]dhcp snooping ?
  binding  DHCP snooping entries
  enable   Enable DHCP snooping

[Comware7]dhcp snooping enable ?
  <cr>

[Comware7]dhcp snooping enable


[Comware7]dhcp snooping binding database filename url tftp://10.0.100.111/Comware7_dhcp.txt


[Comware7]interface g1/0/6

[Comware7-GigabitEthernet1/0/6]dhcp snooping ?
  binding           DHCP snooping entries
  check             Check DHCP packets
  deny              Specify this port as a DHCP packet blocking port
  information       DHCP snooping information
  max-learning-num  Set the maximum number of dynamic DHCP snooping entries
                    allowed on the interface
  rate-limit        Rate limit incoming DHCP traffic
  trust             Specify this port as a trusted port

[Comware7-GigabitEthernet1/0/6]dhcp snooping trust ?
  <cr>

[Comware7-GigabitEthernet1/0/6]dhcp snooping trust


[Comware7-GigabitEthernet1/0/6]dhcp snooping information ?
  circuit-id  Configure the Circuit ID
  enable      Enable the DHCP snooping to support Option 82
  remote-id   Configure the Remote ID
  strategy    Specify the strategy to process Option 82


[Comware7-GigabitEthernet1/0/6]dhcp snooping information enable ?
  <cr>

[Comware7-GigabitEthernet1/0/6]dhcp snooping information remote-id ?
  normal   Specify the normal padding format
  string   Specify the content of the Remote ID
  sysname  Use device name as Remote ID
  vlan     VLAN configuration

[Comware7-GigabitEthernet1/0/6]dhcp snooping information strategy ?
  drop     Drop the DHCP requests containing Option 82
  keep     Forward the DHCP requests without changing Option 82
  replace  Forward the DHCP requests after replacing the original Option 82
```

```
[Comware7]interface g1/0/4

[Comware7-GigabitEthernet1/0/4]dhcp snooping binding record


[Comware7]display dhcp snooping ?
  binding      DHCP snooping entries
  information  Configure the snooping information option
  packet       DHCP packets
  trust        Display information about trusted ports

[Comware7]display dhcp snooping binding
 1 DHCP snooping entries found.
 IP address      MAC address    Lease        VLAN  SVLAN Interface
 =============== ============== ============ ===== ===== =================
 10.1.220.104    e069-9578-4883 86284        220   N/A   GE1/0/4


[Comware7]display dhcp snooping trust
 DHCP snooping is enabled.
 Interface                                        Trusted
 =========================                        ============
 GigabitEthernet1/0/6                             Trusted


[Comware7]display dhcp snooping binding database
 File name               :   tftp://10.0.100.111/Comware7_dhcp.txt
 Username                :
 Password                :
 Update interval         :   300 seconds
 Latest write time       :   May 17 17:01:01 2015
 Status                  :   Last write succeeded.


[Comware7]display dhcp snooping packet statistics
 DHCP packets received                  : 38
 DHCP packets sent                      : 3
 Invalid DHCP packets dropped           : 0
```

Cisco

```
Cisco(config)#ip dhcp snooping ?
  database     DHCP snooping database agent
  information  DHCP Snooping information
  verify       DHCP snooping verify
  vlan         DHCP Snooping vlan
  <cr>


Cisco(config)#ip dhcp snooping


Cisco(config)#ip dhcp snooping database tftp://10.0.100.111/Cisco_dhcp.txt


Cisco(config)#ip dhcp snooping information ?
  option  DHCP Snooping information option


Cisco(config)#ip dhcp snooping information option ?
  allow-untrusted  DHCP Snooping information option allow-untrusted
  format           Option 82 information format
  <cr>
```

```
Cisco(config)#ip dhcp snooping information option allow-untrusted ?
  <cr>


Cisco(config)#ip dhcp snooping information option format ?
  remote-id  Remote id option 82 format

Cisco(config)#ip dhcp snooping information option format remote-id ?
  hostname  Use configured hostname for remote id
  string    User defined string for remote id


Cisco(config)#ip dhcp snooping verify ?
  mac-address             DHCP snooping verify mac-address
  no-relay-agent-address  DHCP snooping verify giaddr

Cisco(config)#ip dhcp snooping verify mac-address ?
  <cr>

Cisco(config)#ip dhcp snooping verify no-relay-agent-address ?
  <cr>


Cisco(config)#ip dhcp snooping vlan ?
  WORD  DHCP Snooping vlan first number or vlan range, example: 1,3-5,7,9-11

Cisco(config)#ip dhcp snooping vlan 220


Cisco(config)#interface g1/0/6

Cisco(config-if)#ip dhcp snooping ?
  information  DHCP Snooping information
  limit        DHCP Snooping limit
  trust        DHCP Snooping trust config
  vlan         DHCP Snooping vlan

Cisco(config-if)#ip dhcp snooping trust


Cisco#show ip dhcp snooping ?
  binding     DHCP snooping bindings
  database    DHCP snooping database agent
  statistics  DHCP snooping statistics
  |           Output modifiers
  <cr>

Cisco#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
220
DHCP snooping is operational on following VLANs:
220
Smartlog is configured on following VLANs:
none
Smartlog is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
```

```
   remote-id: 0022.91ab.4380 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
GigabitEthernet1/0/6       yes        yes             unlimited
  Custom circuit-ids:


Cisco#show ip dhcp snooping database
Agent URL : tftp://10.0.100.111/Cisco_dhcp.txt
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 164 (00:02:44)
Abort Timer Expiry : Not Running

Last Succeded Time : 18:03:54 US-Cent Sun May 17 2015
Last Failed Time : 17:59:18 US-Cent Sun May 17 2015
Last Failed Reason : Expected more data on read.

Total Attempts       :        7   Startup Failures :        2
Successful Transfers :        2   Failed Transfers :        5
Successful Reads     :        1   Failed Reads     :        3
Successful Writes    :        1   Failed Writes    :        0
Media Failures       :        0



Cisco#show ip dhcp snooping statistics detail
 Packets Processed by DHCP Snooping                    = 2
 Packets Dropped Because
   IDB not known                                       = 0
   Queue full                                          = 0
   Interface is in errdisabled                         = 0
   Rate limit exceeded                                 = 0
   Received on untrusted ports                         = 0
   Nonzero giaddr                                      = 0
   Source mac not equal to chaddr                      = 0
   No binding entry                                    = 0
   Insertion of opt82 fail                             = 0
   Unknown packet                                      = 0
   Interface Down                                      = 0
   Unknown output interface                            = 0
   Misdirected Packets                                 = 0
   Packets with Invalid Size                           = 0
   Packets with Invalid Option                         = 0
```

Chapter 33 ARP Protection, ARP Detection, and Dynamic ARP Inspection

This chapter compares commands designed to secure Address Resolution Protocol (ARP). Note that you must enable Dynamic Host Configuration Protocol (DHCP) snooping for ARP protection, ARP detection, and dynamic ARP inspection to operate.

On the VLAN interfaces of a routing switch, dynamic ARP protection ensures that only valid ARP requests and responses are relayed or used to update the local ARP cache. The switch discards ARP packets with invalid IP-to-MAC address bindings advertised in the source protocol address and source physical address fields.

ARP requests are ordinarily broadcast and received by all devices in a broadcast domain. Most ARP devices update their IP-to-MAC address entries each time they receive an ARP packet even if they did not request the information. This behavior makes an ARP cache vulnerable to attacks.

Because ARP allows a node to update its cache entries on other systems by broadcasting or unicasting a gratuitous ARP reply, an attacker can send his own IP-to-MAC address binding in the reply that causes all traffic destined for a VLAN node to be sent to the attacker's MAC address. As a result, the attacker can intercept traffic for other hosts in a classic "man-in-the-middle" attack. The attacker gains access to any traffic sent to the poisoned address and can capture passwords, e-mail, and Voice over IP (VoIP) calls or even modify traffic before resending it.

Another way attackers can poison the ARP cache of known IP addresses and associated MAC addresses is through unsolicited ARP responses. For example, an attacker can associate the IP address of the network gateway with the MAC address of a network node. In this way, the attacker prevents all outgoing traffic from leaving the network, because the node does not have access to outside networks. As a result, the node is overwhelmed by outgoing traffic destined to another network.

Dynamic ARP protection is designed to protect your network against ARP poisoning attacks in the following ways:

- It allows you to differentiate between trusted and untrusted ports.
- It intercepts all ARP requests and responses on untrusted ports before forwarding them.
- It verifies IP-to-MAC address bindings on untrusted ports with the information stored in the lease database maintained by DHCP snooping and user-configured static bindings (in non-DHCP environments):
    - If a binding is valid, the switch updates its local ARP cache and forwards the packet.
    - If a binding is invalid, the switch drops the packet, preventing other network devices from receiving the invalid IP-to-MAC information.

DHCP snooping intercepts and examines DHCP packets received on switch ports before forwarding the packets. DHCP packets are checked against a database of DHCP binding information. Each binding consists of a client MAC address, port number, VLAN identifier, leased IP address, and lease time. Other security features on the switch use the DHCP binding database to validate packets.

If you have already enabled DHCP snooping on a switch, you may also want to add static IP-to-MAC address bindings to the DHCP snooping database so that ARP packets from devices that have been assigned static IP addresses are also verified.

ARP packets that contain invalid IP addresses or MAC addresses in their body that do not match the addresses in the Ethernet header are dropped.

When dynamic ARP protection is enabled, only ARP request and reply packets with valid IP-to-MAC address bindings in their packet header are relayed and used to update the ARP cache.

ArubaOS-Switch	Comware5	Cisco
ArubaOS-Switch(config)# dhcp-snooping	[Comware5]dhcp-snooping	Cisco(config)#ip dhcp snooping
ArubaOS-Switch(config)# arp-protect		
ArubaOS-Switch(config)# arp-protect vlan 220	[Comware5]vlan 220 [Comware5-vlan220]arp detection enable	Cisco(config)#ip arp inspection vlan 220
ArubaOS-Switch(config)# arp-protect trust 1	[Comware5]interface g1/0/6	Cisco(config)#interface g1/0/6
	[Comware5-GigabitEthernet1/0/6]arp detection trust	Cisco(config-if)#ip arp inspection trust
ArubaOS-Switch# show arp-protect	[Comware5]display arp detection	Cisco#show ip arp inspection
ArubaOS-Switch# show arp-protect statistics 220	[Comware5]display arp detection statistics	Cisco#show ip arp inspection interfaces
ArubaOS-Switch(config)#ip arp-throttle enable		Cisco(config)#ip tcp intercept list access list number
ArubaOS-Switch(config)#ip arp-throttle exclude-mac <MAC-ADDR-List>		Cisco(config)# ip tcp intercept mode {intercept | watch}
ArubaOS-Switch(config)#ip arp-throttle remediation-mode { monitor | filter }		Cisco(config)# ip tcp intercept drop-mode {oldest | random}
ArubaOS-Switch(config)#ip arp-throttle aging-time <Seconds>		Cisco(config)# ip tcp intercept watch-timeout seconds

ArubaOS-Switch(config)#ip arp-throttle threshold <Packet-Count>		Cisco(config)# ip tcp intercept max-incomplete low number high count
ArubaOS-Switch(config)#show ip arp-throttle		Cisco(config)#show tcp internet connections
	Comware7	
	[Comware7] dhcp snooping enable	
	[Comware7]vlan 220 [Comware7-vlan220]arp detection enable	
	[Comware7]interface g1/0/6	
	[Comware7-GigabitEthernet1/0/6]arp detection trust	
	[Comware7]display arp detection	
	[Comware7]display arp detection statistics	

ArubaOS-Switch

```
ArubaOS-Switch(config)# dhcp-snooping

ArubaOS-Switch(config)# arp-protect ?
 trust                  Configure port(s) as trusted or untrusted.
 validate               Configure additional ARP Protection validation checks.
 vlan                   Enable/disable Dynamic ARP Protection on a VLAN(s).
 <cr>

ArubaOS-Switch(config)# arp-protect

ArubaOS-Switch(config)# arp-protect vlan 220


ArubaOS-Switch(config)# arp-protect trust 1


ArubaOS-Switch# show arp-protect ?
 statistics
 <cr>

ArubaOS-Switch# show arp-protect

 ARP Protection Information

  ARP Protection Enabled : Yes
  Protected Vlans  : 220
  Validate         :

  Port  Trust
  ----- -----
  1     Yes
```

```
  Ports 2-18,25-26,Trk1-Trk3 are untrusted

ArubaOS-Switch# show arp-protect statistics ?
 VLAN-ID-RANGE         Enter a VLAN identifier, a VLAN name or a VLAN range.

ArubaOS-Switch# show arp-protect statistics 220

 ARP Protection Counters for VLAN 220


  ARPs forwarded  : 0           Bad Sender/Target IP          : 0
  Bad bindings    : 0           Source/Sender MAC mismatches  : 0
  Malformed pkts  : 0           Dest/Target   MAC mismatches  : 0
```

Comware5

```
[Comware5]dhcp-snooping


[Comware5]vlan 220

[Comware5-vlan220]arp ?
  detection  Specify ARP detection function
  restricted-forwarding  Restrict ARP packet forwarding

[Comware5-vlan220]arp detection ?
  enable  Enable ARP detection function

[Comware5-vlan220]arp detection enable ?
  <cr>

[Comware5-vlan220]arp detection enable


[Comware5]interface g1/0/6

[Comware5-GigabitEthernet1/0/6]arp ?
  detection         Specify ARP detection function
  filter            Filter ARP packets
  max-learning-num  Set the maximum number of dynamic arp entries learned on
                    the interface
  rate-limit        Limit ARP packet rate

[Comware5-GigabitEthernet1/0/6]arp detection ?
  trust  Specify port trust state

[Comware5-GigabitEthernet1/0/6]arp detection trust ?
  <cr>

[Comware5-GigabitEthernet1/0/6]arp detection trust


[Comware5]display arp detection ?
  statistics  Display ARP detection statistics
  |           Matching output
  <cr>

[Comware5]display arp detection
 ARP detection is enabled in the following VLANs:
 220

 ARP detection:
```

```
[Comware5]display arp detection statistics ?
  interface  Display statistics by interface
  |          Matching output
  <cr>

[Comware5]display arp detection statistics
State: U-Untrusted  T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)           IP            Src-MAC       Dst-MAC       Inspect
BAGG1(U)                   0             0             0             0
GE1/0/1(U)                 0             0             0             0
GE1/0/2(U)                 0             0             0             0
GE1/0/3(U)                 0             0             0             0
GE1/0/4(U)                 0             0             0             2
GE1/0/5(U)                 0             0             0             0
GE1/0/6(T)                 0             0             0             0
GE1/0/7(U)                 0             0             0             0
GE1/0/8(U)                 0             0             0             0
GE1/0/9(U)                 0             0             0             0
GE1/0/10(U)                0             0             0             0
GE1/0/11(U)                0             0             0             0
GE1/0/12(U)                0             0             0             0
GE1/0/13(U)                0             0             0             0
GE1/0/14(U)                0             0             0             0
GE1/0/15(U)                0             0             0             0
GE1/0/16(U)                0             0             0             0
GE1/0/17(U)                0             0             0             0
GE1/0/18(U)                0             0             0             0
GE1/0/19(U)                0             0             0             0
GE1/0/20(U)                0             0             0             0
GE1/0/21(U)                0             0             0             0
GE1/0/22(U)                0             0             0             0
GE1/0/23(U)                0             0             0             0
GE1/0/24(U)                0             0             0             0
GE1/0/25(U)                0             0             0             0
GE1/0/26(U)                0             0             0             0
GE1/0/27(U)                0             0             0             0
GE1/0/28(U)                0             0             0             0
```

Comware7

```
[Comware7]dhcp snooping enable


[Comware7]vlan 220

[Comware7-vlan220]arp ?
  detection              Specify ARP detection function
  fast-reply             Specify ARP fast reply function
  restricted-forwarding  Specify restrict ARP packet forwarding function
  snooping               Specify ARP snooping function

[Comware7-vlan220]arp detection ?
  enable  Enable ARP detection function

[Comware7-vlan220]arp detection enable ?
  <cr>

[Comware7-vlan220]arp detection enable


[Comware7]interface g1/0/6
```

```
[Comware7-GigabitEthernet1/0/6]arp ?
  detection         Specify ARP detection function
  filter            Filter ARP packets
  max-learning-num  Set the maximum number of dynamic ARP entries learned on the
                    interface
  rate-limit        Specify ARP packet rate limit

[Comware7-GigabitEthernet1/0/6]arp detection ?
  trust  Configure the port as an ARP detection trusted port

[Comware7-GigabitEthernet1/0/6]arp detection trust ?
  <cr>

[Comware7-GigabitEthernet1/0/6]arp detection trust


[Comware7]display arp detection ?
  >           Redirect it to a file
  >>          Redirect it to a file in append mode
  statistics  Statistics of ARP detection
  |           Matching output
  <cr>

[Comware7]display arp detection
 ARP detection is enabled in the following VLANs:
 220

[Comware7]display arp detection statistics ?
  >          Redirect it to a file
  >>         Redirect it to a file in append mode
  interface  Specify the interface
  |          Matching output
  <cr>



[Comware7]display arp detection statistics
State: U-Untrusted  T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)            IP        Src-MAC   Dst-MAC   Inspect
BAGG1(U)                    0         0         0         0
FGE1/0/53(U)                0         0         0         0
FGE1/0/54(U)                0         0         0         0
GE1/0/1(U)                  0         0         0         0
GE1/0/2(U)                  0         0         0         0
GE1/0/3(U)                  0         0         0         0
GE1/0/4(U)                  0         0         0         0
GE1/0/5(U)                  0         0         0         0
GE1/0/6(T)                  0         0         0         1
GE1/0/7(U)                  0         0         0         0
GE1/0/8(U)                  0         0         0         0
GE1/0/9(U)                  0         0         0         0
GE1/0/10(U)                 0         0         0         0
GE1/0/11(U)                 0         0         0         0
GE1/0/12(U)                 0         0         0         0
GE1/0/13(U)                 0         0         0         0
GE1/0/14(U)                 0         0         0         0
GE1/0/15(U)                 0         0         0         0
GE1/0/16(U)                 0         0         0         0
GE1/0/17(U)                 0         0         0         0
GE1/0/18(U)                 0         0         0         0
GE1/0/19(U)                 0         0         0         0
GE1/0/20(U)                 0         0         0         0
```

```
GE1/0/21(U)                    0          0          0          0
GE1/0/22(U)                    0          0          0          0
GE1/0/23(U)                    0          0          0          0
GE1/0/24(U)                    0          0          0          0
GE1/0/25(U)                    0          0          0          0
GE1/0/26(U)                    0          0          0          0
GE1/0/27(U)                    0          0          0          0
GE1/0/28(U)                    0          0          0          0
GE1/0/29(U)                    0          0          0          0
GE1/0/30(U)                    0          0          0          0
GE1/0/31(U)                    0          0          0          0
GE1/0/32(U)                    0          0          0          0
GE1/0/33(U)                    0          0          0          0
GE1/0/34(U)                    0          0          0          0
GE1/0/35(U)                    0          0          0          0
GE1/0/36(U)                    0          0          0          0
GE1/0/37(U)                    0          0          0          0
GE1/0/38(U)                    0          0          0          0
GE1/0/39(U)                    0          0          0          0
GE1/0/40(U)                    0          0          0          0
GE1/0/41(U)                    0          0          0          0
GE1/0/42(U)                    0          0          0          0
GE1/0/43(U)                    0          0          0          0
GE1/0/44(U)                    0          0          0          0
GE1/0/45(U)                    0          0          0          0
GE1/0/46(U)                    0          0          0          0
GE1/0/47(U)                    0          0          0          0
GE1/0/48(U)                    0          0          0          0
XGE1/0/49(U)                   0          0          0          0
XGE1/0/50(U)                   0          0          0          0
XGE1/0/51(U)                   0          0          0          0
XGE1/0/52(U)                   0          0          0          0
```

Cisco

```
Cisco(config)#ip dhcp snooping


Cisco(config)#ip arp inspection ?
  filter      Specify ARP acl to be applied
  log-buffer  Log Buffer Configuration
  smartlog    Smartlog all the logged pkts
  validate    Validate addresses
  vlan        Enable/Disable ARP Inspection on vlans

Cisco(config)#ip arp inspection vlan 220


Cisco(config)#interface g1/0/6

Cisco(config-if)#ip arp ?
  inspection  Arp Inspection configuration

Cisco(config-if)#ip arp inspection ?
  limit  Configure Rate limit of incoming ARP packets
  trust  Configure Trust state

Cisco(config-if)#ip arp inspection trust ?
  <cr>

Cisco(config-if)#ip arp inspection trust


Cisco#show ip arp inspection ?
```

```
  interfaces  Interface status
  log         Log Buffer
  statistics  Packet statistics on DAI configured vlans
  vlan        Selected vlan range
  |           Output modifiers
  <cr>

Cisco# show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
  220     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
  220     Deny             Deny              Off

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
  220             15              1              1              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
  220              0              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
  220                   0                        0                       0


Cisco#show ip arp inspection interfaces ?
  FastEthernet        FastEthernet IEEE 802.3
  GigabitEthernet     GigabitEthernet IEEE 802.3z
  Port-channel        Ethernet Channel of interfaces
  TenGigabitEthernet  Ten Gigabit Ethernet
  |                   Output modifiers
  <cr>

Cisco#show ip arp inspection interfaces

 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Gi1/0/1          Untrusted               15                 1
 Gi1/0/2          Untrusted               15                 1
 Gi1/0/3          Untrusted               15                 1
 Gi1/0/4          Untrusted               15                 1
 Gi1/0/5          Untrusted               15                 1
 Gi1/0/6          Trusted                None               N/A
 Gi1/0/7          Untrusted               15                 1
 Gi1/0/8          Untrusted               15                 1
 Gi1/0/9          Untrusted               15                 1
 Gi1/0/10         Untrusted               15                 1
 Gi1/0/11         Untrusted               15                 1
 Gi1/0/12         Untrusted               15                 1
 Gi1/0/13         Untrusted               15                 1
 Gi1/0/14         Untrusted               15                 1
 Gi1/0/15         Untrusted               15                 1
 Gi1/0/16         Untrusted               15                 1
 Gi1/0/17         Untrusted               15                 1
```

```
Gi1/0/18          Untrusted                15                  1
Gi1/0/19          Untrusted                15                  1
Gi1/0/20          Untrusted                15                  1
Gi1/0/21          Untrusted                15                  1
Gi1/0/22          Untrusted                15                  1
Gi1/0/23          Untrusted                15                  1
Gi1/0/24          Untrusted                15                  1
Gi1/0/25          Untrusted                15                  1
Gi1/0/26          Untrusted                15                  1
Gi1/0/27          Untrusted                15                  1
Gi1/0/28          Untrusted                15                  1
Te1/0/1           Untrusted                15                  1
Te1/0/2           Untrusted                15                  1
Po1               Untrusted                15                  1
```

Chapter 34 Connection Rate Filtering

ArubaOS-Switch provides a feature called connection rate filtering, which is based on HP's Virus Throttle™ technology. Connection rate filtering detects hosts that are generating IP traffic typical of viruses or worms and either throttles or drops all IP traffic from the offending hosts. (For more information, see the HP Switch Software - Access Security Guide for your HP switch.)

Comware and Cisco do not support this exact feature. However, their Address Resolution Protocol (ARP) commands provide rate limiting capabilities for incoming ARP packets.

ArubaOS-Switch	Comware5	Cisco
	No exact Comware5 feature compared to this ArubaOS-Switch feature. Comware5's ARP Attack Protection feature provides rate limiting capability of incoming ARP packets.	No exact Cisco feature compared to this ArubaOS-Switch feature. Cisco's Dynamic ARP Inspection provides rate limiting capability of incoming ARP packets.
`ArubaOS-Switch(config)# connection-rate-filter sensitivity medium`	`[Comware5]arp source-suppression enable`	`Cisco(config-if)#interface g1/0/20`
`ArubaOS-Switch(config)# filter connection-rate 7 notify-only`	`[Comware5]arp source-suppression limit 15`	`Cisco(config-if)#ip arp inspection limit rate 100`
`ArubaOS-Switch(config)# filter connection-rate 10 block`	`[Comware5-GigabitEthernet1/0/20]arp rate-limit rate 75 drop`	
`ArubaOS-Switch(config)# filter connection-rate 17 throttle`		
`ArubaOS-Switch# show connection-rate-filter`	`[Comware5]display arp source-suppression`	`Cisco#show ip arp inspection interfaces`
	Comware7	
	No exact Comware7 feature compared to this ArubaOS-Switch feature. Comware7's ARP Attack Protection feature provides rate limiting capability of incoming ARP packets.	
	`[Comware7]arp source-suppression enable`	
	`[Comware7]arp source-suppression limit 15`	
	`[Comware7-GigabitEthernet1/0/20]arp rate-limit rate 75`	
	`[Comware7]display arp source-suppression`	

```
ArubaOS-Switch(config)# connection-rate-filter ?
 sensitivity           Sets the level of filtering required
 unblock               Resets a host previously blocked by the connection rate filter

ArubaOS-Switch(config)# connection-rate-filter sensitivity
 low                   Sets the level of connection rate filtering to low (most
                       permissive)
 medium                Sets the level of connection rate filtering to medium (permissive)
 high                  Sets the level of connection rate filtering to high (restrictive)
 aggressive            Sets the level of connection rate filtering to aggressive (most
                       restrictive)

ArubaOS-Switch(config)# connection-rate-filter sensitivity medium


ArubaOS-Switch(config)# filter connection-rate ?
 [ethernet] PORT-LIST

ArubaOS-Switch(config)# filter connection-rate 7 ?
 block                 Deny network access until an administrator explicitly re-enables
                       access.
 notify-only           Log an event, but do not deny network access.
 throttle              Deny network access for a period of time and then automatically
                       re-enable access.

ArubaOS-Switch(config)# filter connection-rate 7 notify-only ?
 <cr>

ArubaOS-Switch(config)# filter connection-rate 10 block ?
 <cr>

ArubaOS-Switch(config)# filter connection-rate 17 throttle ?
 <cr>


ArubaOS-Switch# show connection-rate-filter
 all-hosts             Show blocked and throttled IP addresses.
 blocked-hosts         Show blocked IP addresses.
 throttled-hosts       Show throttled IP addresses.
 <cr>

ArubaOS-Switch# show connection-rate-filter

 Connection Rate Filter Configuration

  Global Status:    Enabled
  Sensitivity:      Medium

  Port         | Filter Mode
  -------------+------------------
  7            | NOTIFY-ONLY
  10           | BLOCK
  17           | THROTTLE
```

Comware5

No exact Comware5 feature compared to this ArubaOS-Switch feature.

Comware5's ARP Attack Protection feature provides rate limiting capability of incoming ARP packets.

```
[Comware5]arp ?
  anti-attack         Specify ARP anti-attack function
  check               Specify ARP item check status
```

```
  detection           Specify ARP detection function
  fixup               Specify ARP fixed function
  ip-conflict         IP address conflict
  rate-limit          Limit ARP packet rate
  resolving-route     Specify ARP resolving-route function
  source-suppression  Specify ARP source suppression
  static              Static ARP entry
  timer               Specify ARP timer

[Comware5]arp source-suppression ?
  enable  Enable ARP source suppression
  limit   Specify ARP source suppression limit information

[Comware5]arp source-suppression enable ?
  <cr>

[Comware5]arp source-suppression enable

[Comware5]arp source-suppression limit ?
  INTEGER<2-1024>  Specify ARP source suppression limit number

[Comware5]arp source-suppression limit 15 ?
  <cr>

[Comware5]arp source-suppression limit 15


[Comware5]interface g1/0/20

[Comware5-GigabitEthernet1/0/20]arp ?
  detection         Specify ARP detection function
  filter            Filter ARP packets
  max-learning-num  Set the maximum number of dynamic arp entries learned on
                    the interface
  rate-limit        Limit ARP packet rate


[Comware5-GigabitEthernet1/0/20]arp rate-limit ?
  disable  Disable ARP packet rate limit
  rate     Specify ARP packet rate

[Comware5-GigabitEthernet1/0/20]arp rate-limit rate ?
  INTEGER<5-100>  Rate value (packet per second)

[Comware5-GigabitEthernet1/0/20]arp rate-limit rate 75 ?
  drop  Drop ARP packets over limited rate

[Comware5-GigabitEthernet1/0/20]arp rate-limit rate 75 drop ?
  <cr>

[Comware5-GigabitEthernet1/0/20]arp rate-limit rate 75 drop


[Comware5]display arp source-suppression
 ARP source suppression is enabled
 Current suppression limit: 15
 Current cache length: 16
```

Comware7

No exact Comware7 feature compared to this ArubaOS-Switch feature.

Comware7's ARP Attack Protection feature provides rate limiting capability of incoming ARP packets.

```
[Comware7]arp ?
  active-ack           Specify ARP active acknowledgement function
  check                Specify ARP item check status
  detection            Specify ARP detection function
  fixup                Specify ARP fixed function
  ip-conflict          Specify ARP IP address conflict information printing
                       prompt function
  max-learning-number  Set the maximum number of dynamic ARP entries that can be
                       learned
  multiport            Configure a multiport ARP entry
  rate-limit           Specify ARP packet rate limit
  resolving-route      Specify ARP resolving-route function
  source-mac           Specify ARP fixed source MAC address anti-attack function
  source-suppression   Specify ARP source suppression function
  static               Static ARP entry
  timer                Specify ARP timer
  valid-check          Specify ARP valid check function

[Comware7]arp source-suppression ?
  enable  Enable ARP source suppression function
  limit   Specify ARP source suppression limit information

[Comware7]arp source-suppression enable ?
  <cr>

[Comware7]arp source-suppression enable

[Comware7]arp source-suppression limit ?
  INTEGER<2-1024>  Value of limit

[Comware7]arp source-suppression limit 15 ?
  <cr>

[Comware7]arp source-suppression limit 15


[Comware7]interface g1/0/20

[Comware7-GigabitEthernet1/0/20]arp ?
  detection         Specify ARP detection function
  filter            Filter ARP packets
  max-learning-num  Set the maximum number of dynamic ARP entries learned on the
                    interface
  rate-limit        Specify ARP packet rate limit


[Comware7-GigabitEthernet1/0/20]arp rate-limit ?
  disable  Disable ARP packet rate limit
  rate     Specify ARP packet rate

[Comware7-GigabitEthernet1/0/20]arp rate-limit rate ?
  INTEGER<5-200>  Rate value (packet per second)
  <cr>

[Comware7-GigabitEthernet1/0/20]arp rate-limit rate 75 ?
  <cr>

[Comware7-GigabitEthernet1/0/20]arp rate-limit rate 75
```

```
[Comware7]display arp source-suppression
 ARP source suppression is enable
 Current suppression limit: 15
```

Cisco

No specific Cisco feature compared to this ArubaOS-Switch feature.

Cisco's Dynamic ARP Inspection provides rate limiting capability of incoming ARP packets.

```
Cisco(config-if)#interface g1/0/20


Cisco(config-if)#ip arp inspection ?
  limit  Configure Rate limit of incoming ARP packets
  trust  Configure Trust state

Cisco(config-if)#ip arp inspection limit ?
  none  No limit
  rate  Rate Limit

Cisco(config-if)#ip arp inspection limit rate ?
  <0-2048>  Packets per second

Cisco(config-if)#ip arp inspection limit rate 100 ?
  burst  Configure Burst parameters for ARP packets
  <cr>

Cisco(config-if)#ip arp inspection limit rate 100


Cisco#show ip arp inspection interfaces

 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Gi1/0/1          Untrusted               15                 1
 Gi1/0/2          Untrusted               15                 1
 Gi1/0/3          Untrusted               15                 1
 Gi1/0/4          Untrusted               15                 1
 Gi1/0/5          Untrusted               15                 1
 Gi1/0/6          Untrusted               15                 1
 Gi1/0/7          Untrusted               15                 1
 Gi1/0/8          Untrusted               15                 1
 Gi1/0/9          Untrusted               15                 1
 Gi1/0/10         Untrusted               15                 1
 Gi1/0/11         Untrusted               15                 1
 Gi1/0/12         Untrusted               15                 1
 Gi1/0/13         Untrusted               15                 1
 Gi1/0/14         Untrusted               15                 1
 Gi1/0/15         Untrusted               15                 1
 Gi1/0/16         Untrusted               15                 1
 Gi1/0/17         Untrusted               15                 1
 Gi1/0/18         Untrusted               15                 1
 Gi1/0/19         Untrusted               15                 1
 Gi1/0/20         Untrusted              100                 1
 Gi1/0/21         Untrusted               15                 1
 Gi1/0/22         Untrusted               15                 1
 Gi1/0/23         Untrusted               15                 1
 Gi1/0/24         Untrusted               15                 1
 Gi1/0/25         Untrusted               15                 1
 Gi1/0/26         Untrusted               15                 1
```

```
Gi1/0/27          Untrusted                15                  1
Gi1/0/28          Untrusted                15                  1
Te1/0/1           Untrusted                15                  1
Te1/0/2           Untrusted                15                  1
Po1               Untrusted                15                  1
```

Chapter 35 802.1X Authentication

This chapter compares the commands that enforce 802.1X authentication for devices and users accessing the network.

LANs are often deployed in a way that allows unauthorized clients to attach to network devices, or allows unauthorized users to get access to unattended clients on a network. Also, the use of Dynamic Host Configuration Protocol (DHCP) services and zero configuration make access to networking services easily available. This exposes the network to unauthorized use and malicious attacks. Although access to the network should be made easy, uncontrolled and unauthorized access is usually not desirable. 802.1X simplifies security management by providing access control along with the ability to control user profiles from RADIUS servers, while allowing a given user the same access to the network and its resources from multiple points within the network.

Three different types of 802.1X access methods are available, depending on the device types and/or capability as well as the operational use. Traditional 802.1X use requires a software component on the client device known as the supplicant. If the device does not have this software component, authentication via its MAC address can be used (however this is considered not as secure). If authentication to a network is provided to "guest users" and they do not or cannot have a supplicant, then authentication via a web page is possible.

a) 802.1X Authentication

ArubaOS-Switch	Comware	Cisco

`ArubaOS-Switch(config)# radius-server host 10.0.100.111 key password`	`[Comware]radius scheme <radius-auth>`
	
	`[Comware-radius-radius-auth]primary authentication 10.0.100.111 1812`
	
	`[Comware-radius-radius-auth]primary accounting 10.0.100.111 1813`
	
	`[Comware-radius-radius-auth]key authentication password`
	
	`[Comware-radius-radius-auth]user-name-format without-domain`
	
	`[Comware-radius-radius-auth]server-type extended`
	
	(note - the last command above is only for Comware5)
		`Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key password`

`ArubaOS-Switch(config)#radius-server tracking {enable | disable}`		`Cisco(config)#aaa authentication dot1x default group radius`

ArubaOS-Switch(config)#no radius-server tracking user-name		Cisco(config)#no aaa authentication default group radius
ArubaOS-Switch(config)#setmib hpSwitchRadiusTracking.0 -i 1		
ArubaOS-Switch(config)#setmib hpSwitchRadiusTrackingUserName.0 -D "MyTester"		
ArubaOS-Switch(config)# setmib hpSwitchRadiusTrackingUserName.0 -D "11111111111”		
ArubaOS-Switch(config)# aaa authentication port-access eap-radius		Cisco(config)#aaa new-model Cisco(config)#aaa authentication dot1x default group radius Cisco(config)#aaa authorization network default group radius
ArubaOS-Switch(config)# aaa port-access authenticator 14	[Comware]domain 8021x	Cisco(config)#dot1x system-auth-control
ArubaOS-Switch(config)# aaa port-access authenticator 14 unauth-vid 99	[Comware-isp-8021x]authentication lan-access radius-scheme radius-auth	
ArubaOS-Switch(config)# aaa port-access authenticator 14 client-limit 1	[Comware-isp-8021x]authorization lan-access radius-scheme radius-auth	Cisco(config)#interface g1/0/14
	[Comware-isp-8021x]accounting lan-access radius-scheme radius-auth	Cisco(config-if)#switchport mode access
ArubaOS-Switch(config)# aaa port-access authenticator active	[Comware]domain default enable 8021x	Cisco(config-if)#dot1x pae authenticator
	[Comware]dot1x	Cisco(config-if)#authentication host-mode single-host
	[Comware]dot1x authentication-method eap	Cisco(config-if)#authentication port-control auto
	[Comware]interface g1/0/14	Cisco(config-if)#authentication event fail action authorize vlan 99
	[Comware-GigabitEthernet1/0/14]dot1x	
	[Comware-GigabitEthernet1/0/14]undo dot1x handshake	
	[Comware-GigabitEthernet1/0/14]dot1x auth-fail vlan 99	
	[Comware-GigabitEthernet1/0/14]dot1x max-user 1	
	[Comware-GigabitEthernet1/0/14]stp edged-port enable	

ArubaOS-Switch# show port-access authenticator	[Comware]display dot1x sessions	Cisco#show dot1x all summary
ArubaOS-Switch# show port-access authenticator vlan		
ArubaOS-Switch# show vlans ports 14 detail	[Comware]display dot1x interface g1/0/14	Cisco#show dot1x interface g1/0/14 details
ArubaOS-Switch# show vlans 220	[Comware]display interface brief [Comware]display vlan 220	Cisco#show vlan brief
ArubaOS-Switch# show port-access authenticator clients		
ArubaOS-Switch#show authorization feature		Cisco(config)#show users lawful-intercept
ArubaOS-Switch#show authorization feature <name>		
ArubaOS-Switch#show authorization feature <name> detailed		Cisco(config)#command exec include-exclusive show ip interface

ArubaOS-Switch

```
ArubaOS-Switch(config)# radius-server host 10.0.100.111 key password


ArubaOS-Switch(config)# aaa ?
 accounting            Configure accounting parameters on the switch.
 authentication        Configure authentication parameters on the switch.
 authorization         Configure authorization parameters on the switch.
 port-access           Configure 802.1X (Port Based Network Access), MAC address based
                       network access, or web authentication based network access on the
                       device.
 server-group          Place the RADIUS server into the RADIUS server group.

ArubaOS-Switch(config)# aaa authentication ?
 allow-vlan            Configure authenticator ports to apply VLAN changes immediately.
 console               Configure authentication mechanism used to control access to the
                       switch console.
 disable-username      Bypass the username during authentication while accessing the
                       switch to get Manager or Operator access.
 local-user            Create or remove a local user account.
 lockout-delay         The number of seconds after repeated login failures before a user
                       may again attempt login.
 login                 Specify that switch respects the authentication server's privilege
                       level.
 mac-based             Configure authentication mechanism used to control mac-based port
                       access to the switch.
 num-attempts          The number of login attempts allowed.
 port-access           Configure authentication mechanism used to control access to the
                       network.
 ssh                   Configure authentication mechanism used to control SSH access to
                       the switch.
 telnet                Configure authentication mechanism used to control telnet access
                       to the switch.
 web                   Configure authentication mechanism used to control web access to
                       the switch.
 web-based             Configure authentication mechanism used to control web-based port
                       access to the switch.

ArubaOS-Switch(config)# aaa authentication port-access ?
 local                 Use local switch user/password database.
 eap-radius            Use EAP capable RADIUS server.
 chap-radius           Use CHAP (MD5) capable RADIUS server.
```

```
ArubaOS-Switch(config)# aaa authentication port-access eap-radius ?
 none                   Do not use backup authentication methods.
 authorized             Allow access without authentication.
 cached-reauth          Grant access in case of reauthentication retaining the current
                        session attributes.
 server-group           Specify the server group to use.
 <cr>

ArubaOS-Switch(config)# aaa authentication port-access eap-radius


ArubaOS-Switch(config)# aaa port-access ?
 authenticator          Configure 802.1X (Port Based Network Access) authentication on the
                        device or the device's port(s).
 gvrp-vlans             Enable/disable the use of RADIUS-assigned dynamic (GVRP) VLANs.
 local-mac              Configure Local MAC address based network authentication on the
                        device or the device's port(s).
 mac-based              Configure MAC address based network authentication on the device
                        or the device's port(s).
 [ethernet] PORT-LIST   Manage general port security features on the device port(s).
 supplicant             Manage 802.1X (Port Based Network Access) supplicant on the device
                        ports.
 web-based              Configure web authentication based network authentication.


ArubaOS-Switch(config)# aaa port-access authenticator ?
 active                 Activate/deactivate 802.1X authenticator.
 cached-reauth-delay    Set period of time, in seconds, during which authenticator will
                        not initiate reauthentications after a cached reauthentication.
 [ethernet] PORT-LIST   Manage 802.1X on the device port(s).

ArubaOS-Switch(config)# aaa port-access authenticator 14 ?
 auth-vid               Configures VLAN where to move port after successful authentication
                        (not configured by default).
 cached-reauth-period   Time in seconds, during which cached reauthentication is allowed
                        on the port.The minimum reauthentication period should be greater
                        than 30 seconds.
 clear-statistics       Clear the authenticator statistics.
 client-limit           Set the maximum number of clients to allow on the port.With no
                        client limit, authentication happens in port-based mode, otherwise
                        in client-based mode.
 control                Set the authenticator to Force Authorized, Force Unauthorized or
                        Auto state (default Auto).
 initialize             Reinitialize the authenticator state machine.
 logoff-period          Set period of time after which a client will be considered removed
                        from the port for a lack of activity.
 max-requests           Set maximum number of times the switch retransmits authentication
                        requests (default 2).
 quiet-period           Set the period of time the switch does not try to acquire a
                        supplicant (default 60 sec.).
 reauth-period          Set the re-authentication timeout (in seconds, default 0); set to
                        '0' to disable re-authentication.
 reauthenticate         Force re-authentication to happen.
 server-timeout         Set the authentication server response timeout (default 300 sec.).
 supplicant-timeout     Set the supplicant response timeout on an EAP request (default 30
                        sec.).
 tx-period              Set the period of time the switch waits until retransmission of
                        EAPOL PDU (default 30 sec.).
 unauth-period          Set period of time the switch waits for authentication before
                        moving the port to the VLAN for unauthenticated clients.
 unauth-vid             Configures VLAN where to keep port while there is an
                        unauthenticated client connected (not configured by default).
```

```
 <cr>

ArubaOS-Switch(config)# aaa port-access authenticator 14

ArubaOS-Switch(config)# aaa port-access authenticator 14 unauth-vid 99

ArubaOS-Switch(config)# aaa port-access authenticator 14 client-limit 1

ArubaOS-Switch(config)# aaa port-access authenticator active


ArubaOS-Switch# show port-access authenticator ?
 [ethernet] PORT-LIST  Show information for specified ports only.
 clients               Show the current 802.1X client session statistics.
 config                Show 802.1X authenticator configuration.
 session-counters      Show 802.1X current (or last if no current sessions open) sessions
                       counters.
 statistics            Show authentication sessions statistics for 802.1X authenticator.
 vlan                  Show authorized and unauthorized vlans for 802.1X authenticator.
 <cr>

ArubaOS-Switch# show port-access authenticator

 Port Access Authenticator Status

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

       Auths/  Unauth  Untagged Tagged           % In  RADIUS Cntrl
  Port Guests  Clients VLAN     VLANs  Port COS  Limit ACL    Dir   Port Mode
  ---- ------- ------- -------- ------ --------- ----- ------ ----- ----------
  14   1/0     0       220      No     No        No    No     both  1000FDx


ArubaOS-Switch# show port-access authenticator vlan

 Port Access Authenticator VLAN Configuration

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

       Access  Unauth  Auth
  Port Control VLAN ID VLAN ID
  ---- ------- ------- -------
  14   Auto    99      0


ArubaOS-Switch# show vlans ports 14 detail

 Status and Counters - VLAN Information - VLAN 220

  VLAN ID : 220
  Name : test
  Status : Port-based
  Voice : No
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  4                Untagged Learn        Down
  5                Untagged Learn        Up
  6                Tagged   Learn        Down
  11               Tagged   Learn        Up
```

```
  13                Tagged   Learn        Up
  14                802.1x   Learn        Up
  15                Tagged   Learn        Up
  Trk1              Tagged   Learn        Down
  Trk2              Tagged   Learn        Down
  Trk3              Tagged   Learn        Down

  Overridden Port VLAN configuration

  Port   Mode
  ------ ------------
  14     No


ArubaOS-Switch# show vlans 1

 Status and Counters - VLAN Information - VLAN 1

  VLAN ID : 1
  Name : DEFAULT_VLAN
  Status : Port-based
  Voice : No
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  1                Untagged Learn        Up
  2                Untagged Learn        Down
  3                Untagged Learn        Down
  6                Untagged Learn        Down
  7                Untagged Learn        Down
  8                Untagged Learn        Down
  10               Untagged Learn        Down
  11               Untagged Learn        Up
  12               Untagged Learn        Down
  13               Untagged Learn        Up
  15               Untagged Learn        Up
  16               Untagged Learn        Down
  17               Untagged Learn        Down
  18               Untagged Learn        Down
  25               Untagged Learn        Down
  26               Untagged Learn        Down
  Trk1             Untagged Learn        Down
  Trk2             Untagged Learn        Down
  Trk3             Untagged Learn        Down

  Overridden Port VLAN configuration

  Port   Mode
  ------ ------------
  14     Untagged


ArubaOS-Switch# show port-access authenticator clients

 Port Access Authenticator Client Status

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

  Port Client Name           MAC Address   IP Address      Client Status
  ---- --------------------- ------------- --------------- --------------------
  14   user1                 00237d-e73adb 10.1.220.106    Authenticated
```

Comware5

```
[Comware5]radius scheme <radius-auth>

[Comware5-radius-radius-auth]primary authentication 10.0.100.111 1812

[Comware5-radius-radius-auth]primary accounting 10.0.100.111 1813

[Comware5-radius-radius-auth]key authentication password

[Comware5-radius-radius-auth]user-name-format without-domain

[Comware5-radius-radius-auth]server-type extended


[Comware5]domain 8021x

[Comware5-isp-8021x]?
Isp view commands:

  access-limit             Specify access limit of domain
  accounting               Specify accounting scheme
  authentication           Specify authentication scheme
  authorization            Specify authorization scheme
  authorization-attribute  Specify authorization attributes of domain
  cfd                      Connectivity fault detection (IEEE 802.1ag)
  display                  Display current system information
  dscp                     Specify a DSCP value for user packets of this domain
  idle-cut                 Specify idle-cut attribute of domain
  mtracert                 Trace route to multicast source
  ping                     Ping function
  quit                     Exit from current command view
  return                   Exit to User View
  save                     Save current configuration
  self-service-url         Specify self-service URL(Uniform Resource Locator)
                           of domain
  state                    Specify state of domain
  tracert                  Trace route function
  undo                     Cancel current setting

[Comware5-isp-8021x]authentication ?
  default     Specify default AAA configuration
  lan-access  Specify lan-access AAA configuration
  login       Specify login AAA configuration
  portal      Specify portal AAA configuration
  super       Specify super AAA configuration

[Comware5-isp-8021x]authentication lan-access ?
  local          Specify local scheme
  none           Specify none scheme
  radius-scheme  Specify RADIUS scheme

[Comware5-isp-8021x]authentication lan-access radius-scheme ?
  STRING<1-32>  Scheme name

[Comware5-isp-8021x]authentication lan-access radius-scheme radius-auth ?
  local  Specify local scheme
  none   Specify none scheme
  <cr>

[Comware5-isp-8021x]authentication lan-access radius-scheme radius-auth
```

```
[Comware5-isp-8021x]authorization ?
  command     Specify command AAA configuration
  default     Specify default AAA configuration
  lan-access  Specify lan-access AAA configuration
  login       Specify login AAA configuration
  portal      Specify portal AAA configuration

[Comware5-isp-8021x]authorization lan-access ?
  local          Specify local scheme
  none           Specify none scheme
  radius-scheme  Specify RADIUS scheme

[Comware5-isp-8021x]authorization lan-access radius-scheme ?
  STRING<1-32>  Scheme name

[Comware5-isp-8021x]authorization lan-access radius-scheme radius-auth ?
  local  Specify local scheme
  none   Specify none scheme
  <cr>

[Comware5-isp-8021x]authorization lan-access radius-scheme radius-auth


[Comware5-isp-8021x]accounting ?
  command     Specify command AAA configuration
  default     Specify default AAA configuration
  lan-access  Specify lan-access AAA configuration
  login       Specify login AAA configuration
  optional    Optional accounting mode
  portal      Specify portal AAA configuration

[Comware5-isp-8021x]accounting lan-access ?
  local          Specify local scheme
  none           Specify none scheme
  radius-scheme  Specify RADIUS scheme

[Comware5-isp-8021x]accounting lan-access radius-scheme ?
  STRING<1-32>  Scheme name

[Comware5-isp-8021x]accounting lan-access radius-scheme radius-auth ?
  local  Specify local scheme
  none   Specify none scheme
  <cr>

[Comware5-isp-8021x]accounting lan-access radius-scheme radius-auth


[Comware5]domain default enable 8021x


[Comware5]dot1x ?
  authentication-method  Specify system authentication method
  domain-delimiter       Specify a set of domain delimiters
  free-ip                Specify free IP configurations
  guest-vlan             Specify guest vlan configuration information of port
  interface              Specify interface configuration information
  max-user               Specify maximal on-line user number per port
  port-control           Specify port authenticated status
  port-method            Specify port controlled method
  quiet-period           Enable quiet period function
  retry                  Specify maximal request times
  timer                  Specify timer parameters
  url                    Specify URL of the redirection server
```

```
  <cr>

[Comware5]dot1x
 802.1x is enabled globally.

[Comware5]dot1x authentication-method ?
  chap  CHAP(Challenge Handshake Authentication Protocol) authentication
        method. It's default.
  eap   EAP(Extensible Authentication Protocol) authentication method
  pap   PAP(Password Authentication Protocol) authentication method

[Comware5]dot1x authentication-method eap ?
  <cr>

[Comware5]dot1x authentication-method eap
 EAP authentication is enabled


[Comware5]interface g1/0/14

[Comware5-GigabitEthernet1/0/14]dot1x ?
  attempts           Specify 802.1X authentication attempts
  auth-fail          Specify a VLAN for clients failing the 802.1X
                     authentication on the port
  binding-mac        MAC address binding function
  critical           Specify critical vlan configuration
  eapol              EAPOL packet
  guest-vlan         Specify guest vlan configuration information of port
  handshake          Enable handshake with online user(s)
  mandatory-domain   Specify the domain for 802.1X
  max-user           Specify maximal on-line user number per port
  multicast-trigger  Enable multicast trigger at specify interface
  port-control       Specify port authenticated status
  port-method        Specify port controlled method
  re-authenticate    Enable periodic reauthentication of the online user(s)
  unicast-trigger    Enable unicast trigger
  user-ip            User ip address
  voice              Specify voice vlan configuration
  <cr>

[Comware5-GigabitEthernet1/0/14]dot1x
 802.1x is enabled on port GigabitEthernet1/0/14.

[Comware5-GigabitEthernet1/0/14]undo dot1x handshake

[Comware5-GigabitEthernet1/0/14]dot1x auth-fail vlan 99

[Comware5-GigabitEthernet1/0/14]dot1x max-user 1

[Comware5-GigabitEthernet1/0/14]stp edged-port enable


[Comware5]display dot1x ?
  interface   Show information of interfaces
  sessions    Sessions information
  statistics  Statistics information
  |           Matching output
  <cr>

[Comware5]display dot1x sessions
 Equipment 802.1X protocol is enabled
 EAP authentication is enabled
```

```
 The maximum 802.1X user resource number is 1024 per slot
 Total current used 802.1X resource number is 1

 GigabitEthernet1/0/1  is link-down
   802.1X protocol is disabled
   Handshake is enabled
   Handshake secure is disabled
   802.1X unicast-trigger is disabled
   802.1X user-ip freeze is disabled

   Controlled User(s) amount to 0
...
GigabitEthernet1/0/14  is link-up
   802.1X protocol is enabled
   Handshake is disabled
   Handshake secure is disabled
   802.1X unicast-trigger is disabled
   802.1X user-ip freeze is disabled
 1. Authenticated user : MAC address: 0023-7de7-3adb

   Controlled User(s) amount to 1
...


[Comware5]display dot1x interface g1/0/14
 Equipment 802.1X protocol is enabled
 EAP authentication is enabled
 EAD quick deploy is disabled

 Configuration: Transmit Period   30 s,  Handshake Period       15 s
                Quiet Period      60 s,  Quiet Period Timer is disabled
                Supp Timeout      30 s,  Server Timeout        100 s
                Reauth Period   3600 s
                The maximal retransmitting times    2
 EAD quick deploy configuration:
                EAD timeout:   30 m

 The maximum 802.1X user resource number is 1024 per slot
 Total current used 802.1X resource number is 1

 GigabitEthernet1/0/14  is link-up
   802.1X protocol is enabled
   Handshake is disabled
   Handshake secure is disabled
   802.1X unicast-trigger is disabled
   802.1X user-ip freeze is disabled
   Periodic reauthentication is disabled
   The port is an authenticator
   Authentication Mode is Auto
   Port Control Type is Mac-based
   802.1X Multicast-trigger is enabled
   Mandatory authentication domain: NOT configured
   Guest VLAN: NOT configured
   Auth-Fail VLAN: 99
   Critical VLAN: NOT configured
   Critical recovery-action: NOT configured
   Voice VLAN: NOT configured
   Max number of on-line users is 1

   EAPOL Packet: Tx 45, Rx 45
   Sent EAP Request/Identity Packets : 11
        EAP Request/Challenge Packets: 0
        EAP Success Packets: 6, Fail Packets: 0
```

```
   Received EAPOL Start Packets : 6
            EAPOL LogOff Packets: 0
            EAP Response/Identity Packets : 11
            EAP Response/Challenge Packets: 22
            Error Packets: 0
 1. Authenticated user : MAC address: 0023-7de7-3adb

   Controlled User(s) amount to 1


[Comware5]display interface brief
The brief information of interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
Loop0                UP   UP(s)    10.0.0.31
NULL0                UP   UP(s)    --
Vlan1                UP   UP       10.0.111.31
Vlan100              UP   UP       10.1.100.3      test2
Vlan220              UP   UP       10.1.220.3      data
Vlan230              UP   UP       10.1.230.3      voice
Vlan240              UP   UP       10.1.240.3

The brief information of interface(s) under bridge mode:
Link: ADM - administratively down; Stby - standby
Speed or Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
BAGG1                DOWN auto    A      T    1    Trunk-link-to-ArubaOS-Switch
GE1/0/1              ADM  auto    A      A    1    link-to-core
GE1/0/2              DOWN auto    A      A    1
GE1/0/3              DOWN auto    A      A    1
GE1/0/4              UP   100M(a) F(a)   A    220
GE1/0/5              DOWN auto    A      H    220
GE1/0/6              UP   1G(a)   F(a)   T    1
GE1/0/7              DOWN auto    A      A    1
GE1/0/8              DOWN auto    A      A    1
GE1/0/9              DOWN auto    A      A    100
GE1/0/10             DOWN auto    A      A    1
GE1/0/11             DOWN auto    A      A    1
GE1/0/12             DOWN auto    A      A    1
GE1/0/13             DOWN auto    A      A    1
GE1/0/14             UP   1G(a)   F(a)   A    220
GE1/0/15             DOWN auto    A      A    1
GE1/0/16             DOWN auto    A      A    1
GE1/0/17             DOWN auto    A      A    1
GE1/0/18             DOWN auto    A      A    1
GE1/0/19             DOWN auto    A      A    1
GE1/0/20             DOWN auto    A      A    1
GE1/0/21             DOWN auto    A      A    1
GE1/0/22             DOWN auto    A      A    1
GE1/0/23             DOWN auto    A      T    1    LACP-link-to-ArubaOS-Switch
GE1/0/24             DOWN auto    A      T    1    LACP-link-to-ArubaOS-Switch
GE1/0/25             ADM  auto    A      A    1
GE1/0/26             ADM  auto    A      A    1
GE1/0/27             ADM  auto    A      A    1
GE1/0/28             ADM  auto    A      A    1


[Comware5]display vlan 220
 VLAN ID: 220
 VLAN Type: static
 Route Interface: configured
```

```
 IPv4 address: 10.1.220.3
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0220
 Name: test
 Tagged   Ports:
    Bridge-Aggregation1
    GigabitEthernet1/0/6     GigabitEthernet1/0/23    GigabitEthernet1/0/24
 Untagged Ports:
    GigabitEthernet1/0/4     GigabitEthernet1/0/5     GigabitEthernet1/0/14
```

Comware7

```
[Comware7]radius scheme <radius-auth>

[Comware7-radius-radius-auth]primary authentication 10.0.100.111 1812

[Comware7-radius-radius-auth]primary accounting 10.0.100.111 1813

[Comware7-radius-radius-auth]key authentication password

[Comware7-radius-radius-auth]user-name-format without-domain


[Comware7]domain 8021x

[Comware7-isp-8021x]?
Isp view commands:
  accounting                Specify accounting scheme
  authentication            Specify authentication scheme
  authorization             Specify authorization scheme
  authorization-attribute   Configure authorization attributes of the domain
  cfd                       Connectivity Fault Detection (CFD) module
  diagnostic-logfile        Diagnostic log file configuration
  display                   Display current system information
  logfile                   Log file configuration
  monitor                   System monitor
  ping                      Ping function
  quit                      Exit from current command view
  return                    Exit to User View
  save                      Save current configuration
  security-logfile          Security log file configuration
  state                     Specify state of domain
  tracert                   Tracert function
  undo                      Cancel current setting

[Comware7-isp-8021x]authentication ?
  advpn       Specify AAA configuration for ADVPN user
  default     Specify default AAA configuration for all types of users
  ike         Specify AAA configuration for IKE user
  lan-access  Specify AAA configuration for lan-access service
  login       Specify AAA configuration for login user
  portal      Specify AAA configuration for PORTAL user
  ppp         Specify AAA configuration for PPP user
  super       Specify AAA configuration for super user

[Comware7-isp-8021x]authentication lan-access ?
  ldap-scheme    Specify LDAP scheme
  local          Specify local scheme
  none           Specify none scheme
  radius-scheme  Specify RADIUS scheme

[Comware7-isp-8021x]authentication lan-access radius-scheme ?
  STRING<1-32>  Scheme name
```

```
[Comware7-isp-8021x]authentication lan-access radius-scheme radius-auth ?
  local  Specify local scheme
  none   Specify none scheme
  <cr>

[Comware7-isp-8021x]authentication lan-access radius-scheme radius-auth


[Comware7-isp-8021x]authorization ?
  advpn       Specify AAA configuration for ADVPN user
  command     Specify AAA configuration for command service
  default     Specify default AAA configuration for all types of users
  lan-access  Specify AAA configuration for lan-access service
  login       Specify AAA configuration for login user
  portal      Specify AAA configuration for PORTAL user
  ppp         Specify AAA configuration for PPP user

[Comware7-isp-8021x]authorization lan-access ?
  local          Specify local scheme
  none           Specify none scheme
  radius-scheme  Specify RADIUS scheme

[Comware7-isp-8021x]authorization lan-access radius-scheme ?
  STRING<1-32>  Scheme name

[Comware7-isp-8021x]authorization lan-access radius-scheme radius-auth ?
  local  Specify local scheme
  none   Specify none scheme
  <cr>

[Comware7-isp-8021x]authorization lan-access radius-scheme radius-auth


[Comware7-isp-8021x]accounting ?
  advpn       Specify AAA configuration for ADVPN user
  command     Specify AAA configuration for command service
  default     Specify default AAA configuration for all types of users
  lan-access  Specify AAA configuration for lan-access service
  login       Specify AAA configuration for login user
  portal      Specify AAA configuration for PORTAL user
  ppp         Specify AAA configuration for PPP user

[Comware7-isp-8021x]accounting lan-access ?
  local          Specify local scheme
  none           Specify none scheme
  radius-scheme  Specify RADIUS scheme

[Comware7-isp-8021x]accounting lan-access radius-scheme ?
  STRING<1-32>  Scheme name

[Comware7-isp-8021x]accounting lan-access radius-scheme radius-auth ?
  local  Specify local scheme
  none   Specify none scheme
  <cr>

[Comware7-isp-8021x]accounting lan-access radius-scheme radius-auth


[Comware7]domain default enable 8021x


[Comware7]dot1x ?
  authentication-method  Specify an 802.1X authentication
```

```
  domain-delimiter       Specify a set of domain name delimiters
  ead-assistant          Specify the assistant function for the EAD quick
                         employment
  quiet-period           Enable the quiet timer
  retry                  Specify the maximum number of attempts for sending an
                         authentication request
  smarton                Configure the SmartOn function
  timer                  Set 802.1X timers
  <cr>

[Comware7]dot1x

[Comware7]dot1x authentication-method ?
  chap  CHAP(Challenge Handshake Authentication Protocol) authentication
  eap   EAP(Extensible Authentication Protocol) authentication
  pap   PAP(Password Authentication Protocol) authentication

[Comware7]dot1x authentication-method eap ?
  <cr>

[Comware7]dot1x authentication-method eap


[Comware7]interface g1/0/14

[Comware7-GigabitEthernet1/0/14]dot1x ?
  auth-fail          Auth-Fail VLAN configuration
  critical           Critical VLAN configuration
  guest-vlan         Specify a guest VLAN with restricted services for
                     non-authenticated 802.1X users
  handshake          Configure the handshake function
  mandatory-domain   Specify a mandatory 802.1X authentication domain
  max-user           Specify the max number of online 802.1X users
  multicast-trigger  Enable the multicast trigger function on the interface
  port-control       Specify a port control status on the interface
  port-method        Specify a port control method on the interface
  re-authenticate    Configure the periodic re-authentication function
  smarton            Configure the SmartOn function
  unicast-trigger    Enable the unicast trigger function
  <cr>

[Comware7-GigabitEthernet1/0/14]dot1x
 802.1x is enabled on port GigabitEthernet1/0/14.

[Comware7-GigabitEthernet1/0/14]undo dot1x handshake

[Comware7-GigabitEthernet1/0/14]dot1x auth-fail vlan 99

[Comware7-GigabitEthernet1/0/14]dot1x max-user 1

[Comware7-GigabitEthernet1/0/14]stp edged-port


[Comware7]display dot1x ?
  >           Redirect it to a file
  >>          Redirect it to a file in append mode
  connection  Display connection information of online users
  interface   Specify an interface
  sessions    Display 802.1X sessions
  statistics  Display 802.1X statistics
  |           Matching output
  <cr>
```

```
[Comware7]display dot1x sessions
GigabitEthernet1/0/14  is link-up
   Online 802.1X users: 1
           MAC address       Auth state
           0023-7de7-3adb    Authenticated


[Comware7]display dot1x connection
Slot ID: 1
User MAC address: 0023-7de7-3adb
Access interface: GigabitEthernet1/0/14
Username: user1
Authentication domain: 8021x
Authentication method: EAP
Initial VLAN: 1
Authorization untagged VLAN: 220
Authorization tagged VLAN list: N/A
Authorization ACL ID: N/A
Authorization user profile: N/A
Termination action: N/A
Session timeout period: N/A
Online from: 2015/05/19 14:50:38
Online duration: 0h 5m 12s

Total 1 connections matched.


[Comware7]display dot1x interface g1/0/14
 Global 802.1X parameters:
   802.1X authentication  : Enabled
   EAP authentication     : Enabled
   Max-tx period          : 30 s
   Handshake period       : 15 s
   Quiet timer            : Disabled
       Quiet period       : 60 s
   Supp timeout           : 30 s
   Server timeout         : 100 s
   Reauth period          : 3600 s
   Max auth requests      : 2
   SmartOn supp timeout   : 30 s
   SmartOn retry counts   : 3
   EAD assistant function : Disabled
       EAD timeout        : 30 min
   Domain delimiter       : @
 Max 802.1X users         : 4294967295 per slot
 Online 802.1X users      : 1
 GigabitEthernet1/0/14  is link-up
   802.1X authentication      : Enabled
   Handshake                  : Disabled
   Handshake security         : Disabled
   Unicast trigger            : Disabled
   Periodic reauth            : Disabled
   Port role                  : Authenticator
   Authorization mode         : Auto
   Port access control        : MAC-based
   Multicast trigger          : Enabled
   Mandatory auth domain      : Not configured
   Guest VLAN                 : Not configured
   Auth-Fail VLAN             : 99
   Critical VLAN              : Not configured
   Re-auth server-unreachable : Logoff
   Max online users           : 1
   SmartOn                    : Disabled
```

```
   EAPOL packets: Tx 39, Rx 39
   Sent EAP Request/Identity packets : 10
        EAP Request/Challenge packets: 24
        EAP Success packets: 5
        EAP Failure packets: 0
   Received EAPOL Start packets : 5
            EAPOL LogOff packets: 0
            EAP Response/Identity packets : 10
            EAP Response/Challenge packets: 24
            Error packets: 0
   Online 802.1X users: 1
          MAC address       Auth state
          0023-7de7-3adb    Authenticated


[Comware7]display interface brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
InLoop0              UP   UP(s)    --
Loop0                UP   UP(s)    10.0.0.51
M-GE0/0/0            DOWN DOWN     --
NULL0                UP   UP(s)    --
REG0                 UP   --       --
Vlan1                UP   UP       10.0.111.51
Vlan100              UP   UP       10.1.100.5      test2
Vlan220              UP   UP       10.1.220.5
Vlan230              UP   UP       10.1.230.5      voice
Vlan240              UP   UP       10.1.240.5

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
BAGG1                DOWN auto    A      T    1    LACP-link-to-ArubaOS-Switch
FGE1/0/53            DOWN auto    A      A    1
FGE1/0/54            DOWN auto    A      A    1
GE1/0/1              ADM  auto    A      A    1    link-to-core
GE1/0/2              DOWN auto    A      A    1
GE1/0/3              DOWN auto    A      A    1
GE1/0/4              DOWN auto    A      A    220
GE1/0/5              DOWN auto    A      H    220
GE1/0/6              UP   1G(a)   F(a)   T    1
GE1/0/7              DOWN auto    A      A    1
GE1/0/8              DOWN auto    A      A    1
GE1/0/9              DOWN auto    A      A    100
GE1/0/10             DOWN auto    A      A    1
GE1/0/11             DOWN auto    A      A    1
GE1/0/12             DOWN auto    A      A    1
GE1/0/13             DOWN auto    A      A    1
GE1/0/14             UP   1G(a)   F(a)   A    220
GE1/0/15             DOWN auto    A      A    1
GE1/0/16             DOWN auto    A      A    1
GE1/0/17             DOWN auto    A      A    1
GE1/0/18             DOWN auto    A      A    1
GE1/0/19             DOWN auto    A      A    1
GE1/0/20             DOWN auto    A      A    1
GE1/0/21             DOWN auto    A      A    1
GE1/0/22             DOWN auto    A      A    1
```

```
GE1/0/23              DOWN auto    A      T    1    LACP-link-to-ArubaOS-Switch
GE1/0/24              DOWN auto    A      T    1    LACP-link-to-ArubaOS-Switch
GE1/0/25              DOWN auto    A      A    1
GE1/0/26              DOWN auto    A      A    1
GE1/0/27              DOWN auto    A      A    1
GE1/0/28              DOWN auto    A      A    1
GE1/0/29              DOWN auto    A      A    1
GE1/0/30              DOWN auto    A      A    1
GE1/0/31              DOWN auto    A      A    1
GE1/0/32              DOWN auto    A      A    1
GE1/0/33              DOWN auto    A      A    1
GE1/0/34              DOWN auto    A      A    1
GE1/0/35              DOWN auto    A      A    1
GE1/0/36              DOWN auto    A      A    1
GE1/0/37              DOWN auto    A      A    1
GE1/0/38              DOWN auto    A      A    1
GE1/0/39              DOWN auto    A      A    1
GE1/0/40              DOWN auto    A      A    1
GE1/0/41              DOWN auto    A      A    1
GE1/0/42              DOWN auto    A      A    1
GE1/0/43              DOWN auto    A      A    1
GE1/0/44              DOWN auto    A      A    1
GE1/0/45              DOWN auto    A      A    1
GE1/0/46              DOWN auto    A      A    1
GE1/0/47              DOWN auto    A      A    1
GE1/0/48              DOWN auto    A      A    1
XGE1/0/49             ADM  auto    A      A    1
XGE1/0/50             ADM  auto    A      A    1
XGE1/0/51             DOWN auto    A      A    1
XGE1/0/52             DOWN auto    A      A    1


[Comware7]display vlan 220
 VLAN ID: 220
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 10.1.220.5
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0220
 Name: test
 Tagged ports:
    Bridge-Aggregation1
    GigabitEthernet1/0/6          GigabitEthernet1/0/23
    GigabitEthernet1/0/24
 Untagged ports:
    GigabitEthernet1/0/4          GigabitEthernet1/0/5
    GigabitEthernet1/0/14
```

Cisco

```
Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key password


Cisco(config)#aaa new-model

Cisco(config)#aaa authentication ?
  arap              Set authentication lists for arap.
  attempts          Set the maximum number of authentication attempts
  banner            Message to use when starting login/authentication.
  dot1x             Set authentication lists for IEEE 802.1x.
  enable            Set authentication list for enable.
  eou               Set authentication lists for EAPoUDP
  fail-message      Message to use for failed login/authentication.
  login             Set authentication lists for logins.
```

```
  password-prompt  Text to use when prompting for a password
  ppp              Set authentication lists for ppp.
  sgbp             Set authentication lists for sgbp.
  suppress         Do not send access request for a specific type of user.
  username-prompt  Text to use when prompting for a username

Cisco(config)#aaa authentication dot1x ?
  WORD     Named authentication list (max 31 characters, longer will be
           rejected).
  default  The default authentication list.

Cisco(config)#aaa authentication dot1x default ?
  cache  Use Cached-group
  group  Use Server-group
  local  Use local username authentication.

Cisco(config)#aaa authentication dot1x default group ?
  WORD    Server-group name
  ldap    Use list of all LDAP hosts.
  radius  Use list of all Radius hosts.


Cisco(config)#aaa authentication dot1x default group radius ?
  cache  Use Cached-group
  group  Use Server-group
  local  Use local username authentication.
  <cr>

Cisco(config)#aaa authentication dot1x default group radius


Cisco(config)#aaa authorization ?
  auth-proxy           For Authentication Proxy Services
  cache                For AAA cache configuration
  commands             For exec (shell) commands.
  config-commands      For configuration mode commands.
  configuration        For downloading configurations from AAA server
  console              For enabling console authorization
  credential-download  For downloading EAP credential from Local/RADIUS/LDAP
  exec                 For starting an exec (shell).
  multicast            For downloading Multicast configurations from an AAA
                       server
  network              For network services. (PPP, SLIP, ARAP)
  policy-if            For diameter policy interface application.
  prepaid              For diameter prepaid services.
  radius-proxy         For proxying radius packets
  reverse-access       For reverse access connections
  subscriber-service   For iEdge subscriber services (VPDN etc)
  template             Enable template authorization

Cisco(config)#aaa authorization network ?
  WORD     Named authorization list (max 31 characters, longer will be
           rejected).
  default  The default authorization list.

Cisco(config)#aaa authorization network default ?
  cache             Use Cached-group
  group             Use server-group.
  if-authenticated  Succeed if user has authenticated.
  local             Use local database.
  none              No authorization (always succeeds).

Cisco(config)#aaa authorization network default group ?
```

```
  WORD     Server-group name
  ldap     Use list of all LDAP hosts.
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.

Cisco(config)#aaa authorization network default group radius ?
  cache             Use Cached-group
  group             Use server-group.
  if-authenticated  Succeed if user has authenticated.
  local             Use local database.
  none              No authorization (always succeeds).
  <cr>

Cisco(config)#aaa authorization network default group radius


Cisco(config)#dot1x ?
  credentials          Configure 802.1X credentials profiles
  critical             Set 802.1x Critical Authentication parameters
  guest-vlan           Configure Guest Vlan and 802.1x Supplicant behavior
  logging              Set logging parameters
  supplicant           802.1X supplicant configuration
  system-auth-control  Enable or Disable SysAuthControl
  test                 Configure dot1x test related parameters

Cisco(config)#dot1x system-auth-control


Cisco(config)#interface g1/0/14

Cisco(config-if)#switchport mode access

Cisco(config-if)#dot1x ?
  authenticator   Configure authenticator parameters
  credentials     Credentials profile configuration
  default         Configure Dot1x with default values for this port
  max-reauth-req  Max No. of Reauthentication Attempts
  max-req         Max No. of Retries
  max-start       Max No. of EAPOL-Start requests
  pae             Set 802.1x interface pae type
  supplicant      Configure supplicant parameters
  timeout         Various Timeouts

Cisco(config-if)#dot1x pae ?
  authenticator  Set pae type as Authenticator
  both           Set pae type as both Supplicant and Authenticator
  supplicant     Set pae type as Supplicant

Cisco(config-if)#dot1x pae authenticator ?
  <cr>

Cisco(config-if)#dot1x pae authenticator


Cisco(config-if)#authentication ?
  control-direction  Set the control-direction on the interface
  event              Set action for authentication events
  fallback           Enable the Webauth fallback mechanism
  host-mode          Set the Host mode for authentication on this interface
  linksec            Configure link security parameters
  open               Enable or Disable open access on this port
  order              Add an authentication method to the order list
  periodic           Enable or Disable Reauthentication for this port
```

```
  port-control       Set the port-control value
  priority           Add an authentication method to the priority list
  timer              Set authentication timer values
  violation          Configure action to take on security violations

Cisco(config-if)#authentication host-mode ?
  multi-auth    Multiple Authentication Mode
  multi-domain  Multiple Domain Mode
  multi-host    Multiple Host Mode
  single-host   SINGLE HOST Mode

Cisco(config-if)#authentication host-mode single-host ?
  <cr>

Cisco(config-if)#authentication host-mode single-host

Cisco(config-if)#authentication port-control ?
  auto                PortState set to automatic
  force-authorized    PortState set to AUTHORIZED
  force-unauthorized  PortState set to UnAuthorized

Cisco(config-if)#authentication port-control auto ?
  <cr>

Cisco(config-if)#authentication port-control auto


Cisco(config-if)#authentication event ?
  fail         Configure failed authentication actions/parameters
  linksec      Configure actions for link security events
  no-response  Configure non-responsive host actions
  server       Configure actions for AAA server events

Cisco(config-if)#authentication event fail ?
  action  Required action for authentication event
  retry   Number of times to retry failed authentications

Cisco(config-if)#authentication event fail action ?
  authorize    Authorize the port
  next-method  Move to next authentication method

Cisco(config-if)#authentication event fail action authorize ?
  vlan  Configure Authentication Fail vlan

Cisco(config-if)#authentication event fail action authorize vlan ?
  <1-4094>  Enter a VlanId

Cisco(config-if)#authentication event fail action authorize vlan 99 ?
  <cr>

Cisco(config-if)#authentication event fail action authorize vlan 99


Cisco#show dot1x ?
  all        Show 802.1x information for all interfaces
  interface  Interface information to display
  |          Output modifiers
  <cr>

Cisco#show dot1x all ?
  count       Show total no of authorized and unauthorized clients
  details     Show 802.1x details for all interfaces
  statistics  Show 802.1x statistics for all interfaces
```

```
  summary     Show 802.1x summary for all interfaces
  |           Output modifiers
  <cr>

Cisco#show dot1x all summary
Interface       PAE     Client          Status
-------------------------------------------------------
Gi1/0/14        AUTH    0023.7de7.3adb  AUTHORIZED


Cisco#show dot1x interface g1/0/14 details

Dot1x Info for GigabitEthernet1/0/14
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Dot1x Authenticator Client List
-------------------------------
EAP Method                = PEAP
Supplicant                = 0023.7de7.3adb
Session ID                = 0A000029000000020134B324
    Auth SM State         = AUTHENTICATED
    Auth BEND SM State    = IDLE


Cisco#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                                                Gi1/0/7, Gi1/0/8, Gi1/0/10
                                                Gi1/0/11, Gi1/0/12, Gi1/0/13
                                                Gi1/0/15, Gi1/0/16, Gi1/0/17
                                                Gi1/0/18, Gi1/0/19, Gi1/0/20
                                                Gi1/0/21, Gi1/0/22, Gi1/0/23
                                                Gi1/0/24, Te1/0/1, Te1/0/2
100  VLAN0100                         active    Gi1/0/9
220  VLAN0220                         active    Gi1/0/4, Gi1/0/5, Gi1/0/14
230  VLAN0230                         active    Gi1/0/5
240  VLAN0240                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

b) MAC Authentication

ArubaOS-Switch	Comware	Cisco
ArubaOS-Switch(config)# radius-server host 10.0.100.111 key password	[Comware]radius scheme <radius-auth> [Comware-radius-radius-auth]primary authentication 10.0.100.111 1812 [Comware-radius-radius-auth]primary accounting 10.0.100.111 1813 [Comware-radius-radius-auth]key authentication password [Comware-radius-radius-auth]user-name-format without-domain [Comware-radius-radius-auth]server-type extended (note - the last command above is only for Comware5)	Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key password
ArubaOS-Switch(config)# aaa port-access mac-based 16	[Comware]mac-authentication	Cisco(config)#interface g1/0/16
	[Comware]interface g1/0/16	Cisco(config-if)#switchport mode access
ArubaOS-Switch(config)# aaa port-access mac-based 16 unauth-vid 99	[Comware-GigabitEthernet1/0/16]mac-authentication	Cisco(config-if)#dot1x pae authenticator
	[Comware]mac-authentication domain 8021x	Cisco(config-if)#mab
	[Comware]mac-authentication user-name-format mac-address without-hyphen	Cisco(config-if)#authentication order mab Cisco(config-if)#authentication host-mode single-host Cisco(config-if)#authentication port-control auto Cisco(config-if)#authentication event fail action authorize vlan 99
ArubaOS-Switch# show port-access mac-based config 16	[Comware]display mac-authentication interface g1/0/16	Cisco#show dot1x interface g1/0/16 details
ArubaOS-Switch# show port-access mac-based		Cisco#show authentication interface g1/0/16
ArubaOS-Switch# show port-access mac-based clients		
	[Comware]display mac-authentication	

ArubaOS-Switch

```
ArubaOS-Switch(config)# radius-server host 10.0.100.111 key password

ArubaOS-Switch(config)# aaa port-access ?
 authenticator         Configure 802.1X (Port Based Network Access) authentication on the
                       device or the device's port(s).
 gvrp-vlans            Enable/disable the use of RADIUS-assigned dynamic (GVRP) VLANs.
 local-mac             Configure Local MAC address based network authentication on the
                       device or the device's port(s).
 mac-based             Configure MAC address based network authentication on the device
                       or the device's port(s).
 [ethernet] PORT-LIST  Manage general port security features on the device port(s).
 supplicant            Manage 802.1X (Port Based Network Access) supplicant on the device
                       ports.
 web-based             Configure web authentication based network authentication.

ArubaOS-Switch(config)# aaa port-access mac-based ?
 addr-format           Set the MAC address format to be used in the RADIUS request
                       message (default no-delimiter).
 [ethernet] PORT-LIST  Manage MAC address based network authentication on the device
                       port(s).
 password              Specify the password for the MAC authentication. If in enhanced
                       secure-mode, you will be prompted for the password.
 unauth-redirect       Configure macAuth redirect registration server feature.

ArubaOS-Switch(config)# aaa port-access mac-based 16 ?
 addr-limit            Set the port's maximum number of authenticated MAC addresses
                       (default 1).
 addr-moves            Set whether the MAC can move between ports (default disabled - no
                       moves).
 auth-vid              Configures VLAN where to move port after successful authentication
                       (not configured by default).
 cached-reauth-period  Time in seconds, during which cached reauthentication is allowed
                       on the port.The minimum reauthentication period should be greater
                       than 30 seconds.
 logoff-period         Set the period of time of inactivity that the switch considers an
                       implicit logoff (default 300 seconds).
 max-requests          Set maximum number of times the switch retransmits authentication
                       requests (default 3).
 quiet-period          Set the period of time the switch does not try to authenticate
                       (default 60 seconds).
 reauth-period         Set the re-authentication timeout in seconds; set to '0' to
                       disable re-authentication (default 0).
 reauthenticate        Force re-authentication to happen.
 server-timeout        Set the authentication server response timeout (default 300
                       seconds).
 unauth-period         Set period of time the switch waits before moving the port to the
                       VLAN for unauthenticated clients.
 unauth-vid            Configures VLAN where to keep port while there is an unauthorized
                       client connected (not configured by default).
 <cr>

ArubaOS-Switch(config)# aaa port-access mac-based 16

ArubaOS-Switch(config)# aaa port-access mac-based 16 unauth-vid 99


ArubaOS-Switch# show port-access ?
 [ethernet] PORT-LIST  Show Web/MAC Authentication statistics and configuration.
 authenticator         Show 802.1X (Port Based Network Access) authenticator current
                       status, configuration or last session counters.
 config                Show status of 802.1X, Web Auth, and MAC Auth configurations.
```

```
 local-mac              Show Local MAC Authentication statistics and configuration.
 mac-based              Show MAC Authentication statistics and configuration.
 summary                Show summary configuration information for all ports, including
                        that overridden by RADIUS attributes.
 supplicant             Show 802.1X (Port Based Network Access) supplicant current status
                        and configuration.
 web-based              Show Web Authentication statistics and configuration.

ArubaOS-Switch# show port-access mac-based ?
 [ethernet] PORT-LIST  Specify ports for which MAC Authentication information will be
                        shown.
 clients                Show the connected MAC address information.
 config                 Show the current configuration of MAC Authentication.
 <cr>

ArubaOS-Switch# show port-access mac-based config 16

 Port Access MAC-Based Configuration

  MAC Address Format : no-delimiter
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

  Mac password :


  Unauth Redirect Configuration URL :
  Unauth Redirect Client Timeout (sec) : 1800
  Unauth Redirect Restrictive Filter : Disabled
  Total Unauth Redirect Client Count : 0

                 Client Client Logoff    Re-Auth   Unauth  Auth    Cntrl
  Port   Enabled Limit  Moves  Period    Period    VLAN ID VLAN ID Dir
  ------ ------- ------ ------ --------- --------- ------- ------- -----
  16     Yes     1      No     300       0         99      0       both

ArubaOS-Switch# show port-access mac-based

 Port Access MAC-Based Status

       Auths/  Unauth  Untagged Tagged          % In  RADIUS Cntrl
  Port Guests  Clients VLAN     VLANs  Port COS Limit ACL    Dir   Port Mode
  ---- ------- ------- -------- ------ -------- ----- ------ ----- ----------
  16   1/0     0       220      No     No       No    No     both  100FDx

ArubaOS-Switch# show port-access mac-based clients

 Port Access MAC-Based Client Status

  Port MAC Address   IP Address                             Client Status
  ---- ------------- ------------------------------------- --------------------
  16   e06995-784883 10.1.220.108                          authenticated
```

Comware5

```
[Comware5]radius scheme <radius-auth>

[Comware5-radius-radius-auth]primary authentication 10.0.100.111 1812

[Comware5-radius-radius-auth]primary accounting 10.0.100.111 1813

[Comware5-radius-radius-auth]key authentication password

[Comware5-radius-radius-auth]user-name-format without-domain
```

```
[Comware5-radius-radius-auth]server-type extended

[Comware5]mac-authentication ?
  domain            Specify domain server configuration
  interface         Specify interface configuration information
  timer             Timer configuration
  user-name-format  Specify user name format
  <cr>

[Comware5]mac-authentication
 Mac-auth is enabled globally.

[Comware5]interface g1/0/16

[Comware5-GigabitEthernet1/0/16]mac-authentication ?
  critical    Specify critical vlan configuration
  domain      Specify domain server configuration
  guest-vlan  Specify guest VLAN configuration information
  max-user    Specify maximum number of Mac-auth users allowed to access the
              port
  timer       Timer configuration
  <cr>

[Comware5-GigabitEthernet1/0/16]mac-authentication
 Mac-auth is enabled on port GigabitEthernet1/0/16.

[Comware5]mac-authentication domain 8021x

[Comware5]mac-authentication user-name-format ?
  fixed        Use fixed account
  mac-address  Use user's source MAC address as user name

[Comware5]mac-authentication user-name-format mac-address ?
  with-hyphen     MAC address with '-', just like XX-XX-XX-XX-XX-XX
  without-hyphen  MAC address without '-', just like XXXXXXXXXXXX
  <cr>

[Comware5]mac-authentication user-name-format mac-address without-hyphen ?
  lowercase  In lowercase
  uppercase  In uppercase
  <cr>

[Comware5]mac-authentication user-name-format mac-address without-hyphen


[Comware5]display mac-authentication ?
  interface  Display MAC-authentication interface configuration
  |          Matching output
  <cr>

[Comware5]display mac-authentication interface g1/0/16
MAC address authentication is enabled.
 User name format is MAC address in lowercase,like xxxxxxxxxxxx
 Fixed username:mac
 Fixed password:not configured
         Offline detect period is 300s
         Quiet period is 60s
         Server response timeout value is 100s
         Guest vlan reauthentication timeout value is 30s
         The max allowed user number is 1024 per slot
         Current user number amounts to 1
         Current domain is 8021x
```

```
Silent MAC User info:
         MAC Addr         From Port                    Port Index

GigabitEthernet1/0/16 is link-up
  MAC address authentication is enabled
  Authenticate success: 1, failed: 0
  Max number of on-line users is 256
  Current online user number is 1
         MAC Addr         Authenticate State           Auth Index
         e069-9578-4883   MAC_AUTHENTICATOR_SUCCESS     2


[Comware5]display mac-authentication
MAC address authentication is enabled.
 User name format is MAC address in lowercase,like xxxxxxxxxxxx
 Fixed username:mac
 Fixed password:not configured
         Offline detect period is 300s
         Quiet period is 60s
         Server response timeout value is 100s
         Guest vlan reauthentication timeout value is 30s
         The max allowed user number is 1024 per slot
         Current user number amounts to 1
         Current domain is 8021x
...
GigabitEthernet1/0/16 is link-up
  MAC address authentication is enabled
  Authenticate success: 1, failed: 0
  Max number of on-line users is 256
  Current online user number is 1
         MAC Addr         Authenticate State           Auth Index
         e069-9578-4883   MAC_AUTHENTICATOR_SUCCESS     2
...
```

Comware7

```
[Comware7]radius scheme <radius-auth>

[Comware7-radius-radius-auth]primary authentication 10.0.100.111 1812

[Comware7-radius-radius-auth]primary accounting 10.0.100.111 1813

[Comware7-radius-radius-auth]key authentication password

[Comware7-radius-radius-auth]user-name-format without-domain


[Comware7]mac-authentication ?
  domain            Specify an authentication domain
  timer             Specify the MAC authentication timers
  user-name-format  Set user account format
  <cr>

[Comware7]mac-authentication


[Comware7]interface g1/0/16

[Comware7-GigabitEthernet1/0/16]mac-authentication ?
  critical         Critical VLAN configuration
  domain           Specify an authentication domain
  guest-vlan       Specify a guest VLAN for users who fail MAC authentication
                   when an authentication server is reachable
  host-mode        Set the MAC authentication host mode
```

```
  max-user         Specify the max number of concurrent MAC authentication users
                   on the port
  re-authenticate  Configure the periodic re-authentication function
  timer            Specify the MAC authentication timers
  <cr>

[Comware7-GigabitEthernet1/0/16]mac-authentication


[Comware7]mac-authentication domain 8021x

[Comware7]mac-authentication user-name-format ?
  fixed        Use a shared account for all MAC authentication users
  mac-address  Use MAC-based user accounts for MAC authentication users

[Comware7]mac-authentication user-name-format mac-address ?
  with-hyphen     Hyphenate the MAC address, for example xx-xx-xx-xx-xx-xx
  without-hyphen  Exclude hyphens from the MAC address, for example xxxxxxxxxxxx
  <cr>

[Comware7]mac-authentication user-name-format mac-address without-hyphen ?
  lowercase  Letters in lowercase
  uppercase  Letters in uppercase
  <cr>

[Comware7]mac-authentication user-name-format mac-address without-hyphen


[Comware7]display mac-authentication ?
  interface  Display MAC-authentication interface configuration
  |          Matching output
  <cr>

[Comware7]display mac-authentication connection
Slot ID: 1
User MAC address: e069-9578-4883
Access interface: GigabitEthernet1/0/16
Username: e06995784883
Authentication domain: 8021x
Initial VLAN: 1
Authorization untagged VLAN: 220
Authorization ACL ID: N/A
Authorization user profile: N/A
Termination action: N/A
Session timeout period: N/A
Online from: 2015/05/19 15:18:14
Online duration: 0h 3m 53s

Total 1 connections matched.


[Comware7]display mac-authentication interface g1/0/16
Global MAC authentication parameters:
   MAC authentication     : Enabled
   User name format       : MAC address in lowercase(xxxxxxxxxxxx)
           Username       : mac
           Password       : Not configured
   Offline detect period  : 300 s
   Quiet period           : 60 s
   Server timeout         : 100 s
   Authentication domain  : 8021x
 Max MAC-auth users       : 4294967295 per slot
 Online MAC-auth users    : 1
```

```
 Silent MAC users:
          MAC address       VLAN ID  From port               Port index

 GigabitEthernet1/0/16  is link-up
   MAC authentication         : Enabled
   Authentication domain      : Not configured
   Auth-delay timer           : Disabled
   Re-auth server-unreachable : Logoff
   Guest VLAN                 : Not configured
   Critical VLAN              : Not configured
   Host mode                  : Single VLAN
   Max online users           : 4294967295
   Authentication attempts    : successful 1, failed 0
   Current online users       : 1
          MAC address       Auth state
          e069-9578-4883    Authenticated


[Comware7]display mac-authentication
MAC address authentication is enabled.
 User name format is MAC address in lowercase,like xxxxxxxxxxxx
 Fixed username:mac
 Fixed password:not configured
         Offline detect period is 300s
         Quiet period is 60s
         Server response timeout value is 100s
         Guest vlan reauthentication timeout value is 30s
         The max allowed user number is 1024 per slot
         Current user number amounts to 1
         Current domain is 8021x
...
GigabitEthernet1/0/16 is link-up
  MAC address authentication is enabled
  Authenticate success: 1, failed: 0
  Max number of on-line users is 256
  Current online user number is 1
         MAC Addr         Authenticate State           Auth Index
         e069-9578-4883   MAC_AUTHENTICATOR_SUCCESS     2
...
```

Cisco

```
Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key password


Cisco(config)#interface g1/0/16

Cisco(config-if)#switchport mode access

Cisco(config-if)#dot1x ?
  authenticator   Configure authenticator parameters
  credentials     Credentials profile configuration
  default         Configure Dot1x with default values for this port
  max-reauth-req  Max No. of Reauthentication Attempts
  max-req         Max No. of Retries
  max-start       Max No. of EAPOL-Start requests
  pae             Set 802.1x interface pae type
  supplicant      Configure supplicant parameters
  timeout         Various Timeouts

Cisco(config-if)#dot1x pae ?
  authenticator  Set pae type as Authenticator
  both           Set pae type as both Supplicant and Authenticator
```

```
  supplicant     Set pae type as Supplicant

Cisco(config-if)#dot1x pae authenticator ?
  <cr>

Cisco(config-if)#dot1x pae authenticator


Cisco(config-if)#mab ?
  eap  Use EAP authentication for MAC Auth Bypass
  <cr>

Cisco(config-if)#mab eap ?
  <cr>

Cisco(config-if)#mab


Cisco(config-if)#authentication ?
  control-direction  Set the control-direction on the interface
  event              Set action for authentication events
  fallback           Enable the Webauth fallback mechanism
  host-mode          Set the Host mode for authentication on this interface
  linksec            Configure link security parameters
  open               Enable or Disable open access on this port
  order              Add an authentication method to the order list
  periodic           Enable or Disable Reauthentication for this port
  port-control       Set the port-control value
  priority           Add an authentication method to the priority list
  timer              Set authentication timer values
  violation          Configure action to take on security violations


Cisco(config-if)#authentication order ?
  dot1x    Authentication method "dot1x" allowed
  mab      Authentication method "mab" allowed
  webauth  Authentication method "webauth" allowed

Cisco(config-if)#authentication order mab ?
  dot1x    Authentication method "dot1x" allowed
  webauth  Authentication method "webauth" allowed
  <cr>

Cisco(config-if)#authentication order mab

Cisco(config-if)#authentication host-mode single-host

Cisco(config-if)#authentication port-control auto

Cisco(config-if)#authentication event fail action authorize vlan 99



Cisco#show dot1x ?
  all        Show 802.1x information for all interfaces
  interface  Interface information to display
  |          Output modifiers
  <cr>

Cisco#show dot1x interface g1/0/16 details

Dot1x Info for GigabitEthernet1/0/16
------------------------------------
```

```
PAE                         = AUTHENTICATOR
PortControl                 = AUTO
ControlDirection            = Both
HostMode                    = SINGLE_HOST
QuietPeriod                 = 60
ServerTimeout               = 0
SuppTimeout                 = 30
ReAuthMax                   = 2
MaxReq                      = 2
TxPeriod                    = 30

Dot1x Authenticator Client List Empty


Cisco#show authentication ?
  interface      Shows Auth Manager interface information
  method         The name of the Authentication method
  registrations  Shows Auth Manager registrations
  sessions       Shows Auth Manager session information
  statistics     Statistics for authentications

Cisco#show authentication interface g1/0/16

Client list:
Interface  MAC Address     Method   Domain   Status         Session ID
  Gi1/0/16   e069.9578.4883  mab      DATA     Authz Success  0A000029000000008019590EA

Available methods list:
  Handle  Priority  Name
    3        0      dot1x
    4        1      mab
Runnable methods list:
  Handle  Priority  Name
    4        0      mab
```

c) Web or Portal Authentication

ArubaOS-Switch	Comware5	Cisco
ArubaOS-Switch(config)# radius-server host 10.0.100.111 key password	[Comware5]radius scheme <radius-auth> [Comware5-radius-radius-auth]primary authentication 10.0.100.111 1812 [Comware5-radius-radius-auth]primary accounting 10.0.100.111 1813 [Comware5-radius-radius-auth]key authentication password [Comware5-radius-radius-auth]user-name-format without-domain [Comware5-radius-radius-auth]server-type extended	(note - requires special configuration on the RADIUS server) Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key password Cisco(config)#radius-server attribute 8 include-in-access-req Cisco(config)#radius-server vsa send authentication
ArubaOS-Switch(config)# aaa port-access web-based 18	[Comware5]domain web-auth	Cisco(config)#aaa new-model
ArubaOS-Switch(config)# aaa port-access web-based 18 unauth-vid 99	[Comware5-isp-web-auth]authentication portal radius-scheme radius-auth	Cisco(config)#aaa authentication login default group radius (note, above step is required for web authentication, but will now require RADIUS authentication for console login as well. See manual for options) Cisco(config)#aaa authorization auth-proxy default group radius
ArubaOS-Switch(config)# aaa port-access web-based 18 client-limit 5	[Comware5-isp-web-auth]authorization portal radius-scheme radius-auth	Cisco(config)#ip device tracking
	[Comware5-isp-web-auth]accounting portal radius-scheme radius-auth	Cisco(config)#ip admission name web-auth-rule1 proxy http Cisco(config)#ip admission auth-proxy-banner http
	[Comware5] interface LoopBack 12	Cisco(config)#ip access-list extended web-auth-policy1 Cisco(config-ext-nacl)#permit udp any any

		Cisco(config-ext-nacl)#permit tcp any any eq www Cisco(config-ext-nacl)#deny ip any any
	[Comware5-LoopBack12]ip address 1.1.1.1 255.255.255.255	Cisco(config)#fallback profile fallback1
	[Comware5]interface g1/0/18	Cisco(config-fallback-profile)#ip access-group web-auth-policy1 in
	[Comware5-GigabitEthernet1/0/18]port link-type hybrid	Cisco(config-fallback-profile)#ip admission web-auth-rule1
	[Comware5-GigabitEthernet1/0/18]mac-vlan enable	Cisco(config)#interface g1/0/18
	[Comware5-GigabitEthernet1/0/18]portal local-server enable	Cisco(config-if)#switchport mode access Cisco(config-if)#switchport access vlan 220
	[Comware5-GigabitEthernet1/0/18]portal domain web-auth	Cisco(config-if)#dot1x pae authenticator
	[Comware5-GigabitEthernet1/0/18]portal auth-fail vlan 99	Cisco(config-if)#authentication fallback fallback1 Cisco(config-if)#authentication order webauth Cisco(config-if)#authentication port-control auto
	[Comware5-GigabitEthernet1/0/18]stp edged-port enable	Cisco(config-if)#ip access-group web-auth-policy1 in Cisco(config-if)#ip admission web-auth-rule1
ArubaOS-Switch# show port-access web-based	[Comware5]display portal user all	Cisco#show ip admission cache
ArubaOS-Switch# show port-access web-based clients	[Comware5]display connection access-type portal [Comware5]display connection ucibindex 3	
ArubaOS-Switch# show port-access web-based config 18	[Comware5]display portal connection statistics all	Cisco#show authentication interface g1/0/18

ArubaOS-Switch

```
ArubaOS-Switch(config)# radius-server host 10.0.100.111 key password
```

```
ArubaOS-Switch(config)# aaa port-access ?
 authenticator         Configure 802.1X (Port Based Network Access) authentication on the
                       device or the device's port(s).
 gvrp-vlans            Enable/disable the use of RADIUS-assigned dynamic (GVRP) VLANs.
 local-mac             Configure Local MAC address based network authentication on the
                       device or the device's port(s).
 mac-based             Configure MAC address based network authentication on the device
                       or the device's port(s).
 [ethernet] PORT-LIST  Manage general port security features on the device port(s).
 supplicant            Manage 802.1X (Port Based Network Access) supplicant on the device
                       ports.
 web-based             Configure web authentication based network authentication.

ArubaOS-Switch(config)# aaa port-access web-based ?
 access-denied-message Specify the message to be displayed on the login page when a
                       user's login fails.
 dhcp-addr             Set the base address / mask for the temporary pool used by DHCP
                       (base address default is 192.168.0.0, mask default is 24 -
                       255.255.255.0).
 dhcp-lease            Set the lease length of the IP address issued by DHCP (default
                       10).
 ewa-server            IP address or hostname of the enhanced web authentication server
                       on the device.
 [ethernet] PORT-LIST  Manage web authentication based network authentication on the
                       device port(s).
ArubaOS-Switch(config)# aaa port-access web-based 18 ?
 auth-vid              Configures VLAN port will become a member of after successful
                       authentication (not configured by default).
 cached-reauth-period  Time in seconds, during which cached reauthentication is allowed
                       on the port.The minimum reauthentication period should be greater
                       than 30 seconds.
 client-limit          Set the port's maximum number of authenticated clients (default
                       1).
 client-moves          Set whether the client can move between ports (default disabled -
                       no moves).
 logoff-period         Set the period of time of inactivity that the switch considers an
                       implicit logoff (default 300 seconds).
 max-requests          Set maximum number of times the switch retransmits authentication
                       requests (default 3).
 max-retries           Set number of times a client can enter their credentials before
                       authentication is considered to have failed (default 3).
 quiet-period          Set the period of time the switch does not try to authenticate
                       (default 60 seconds).
 reauth-period         Set the re-authentication timeout in seconds; set to '0' to
                       disable re-authentication (default 0).
 reauthenticate        Force re-authentication to happen.
 redirect-url          Set the URL that the user should be redirected to after successful
                       login (default none), Specify url up to 127 characters length.
 server-timeout        Set the authentication server response timeout (default 300
                       seconds).
 ssl-login             Set whether to enable SSL login (https on port 443) (default
                       disabled).
 unauth-vid            Configures VLAN port is a member of while there is an unauthorized
                       client connected (not configured by default).
 <cr>

ArubaOS-Switch(config)# aaa port-access web-based 18

ArubaOS-Switch(config)# aaa port-access web-based 18 unauth-vid 99

ArubaOS-Switch(config)# aaa port-access web-based 18 client-limit 5
```

```
ArubaOS-Switch# sho port-access ?
 [ethernet] PORT-LIST  Show Web/MAC Authentication statistics and configuration.
 authenticator         Show 802.1X (Port Based Network Access) authenticator current
                       status, configuration or last session counters.
 config                Show status of 802.1X, Web Auth, and MAC Auth configurations.
 local-mac             Show Local MAC Authentication statistics and configuration.
 mac-based             Show MAC Authentication statistics and configuration.
 summary               Show summary configuration information for all ports, including
                       that overridden by RADIUS attributes.
 supplicant            Show 802.1X (Port Based Network Access) supplicant current status
                       and configuration.
 web-based             Show Web Authentication statistics and configuration.

ArubaOS-Switch# sho port-access web-based ?
 [ethernet] PORT-LIST  Specify ports for which Web Authentication information will be
                       shown.
 clients               Show the current web client session statistics.
 config                Show the current configuration of Web Authentication.
 <cr>

ArubaOS-Switch# show port-access web-based

 Port Access Web-Based Status

       Auths/  Unauth  Untagged Tagged          % In  RADIUS Cntrl
  Port Guests  Clients VLAN     VLANs  Port COS Limit ACL    Dir   Port Mode
  ---- ------- ------- -------- ------ -------- ----- ------ ----- ----------
  18   1/0     0       220      No     No       No    No     both  1000FDx


ArubaOS-Switch# show port-access web-based clients

 Port Access Web-Based Client Status

  Port Client Name        MAC Address   IP Address      Client Status
  ---- ------------------ ------------- --------------- --------------------
  18   user1              705ab6-e86783 10.1.220.102    authenticated


ArubaOS-Switch# show port-access web-based config 18

 Port Access Web-Based Configuration

  DHCP Base Address      : 192.168.0.0
  DHCP Subnet Mask       : 255.255.255.0
  DHCP Lease Length      : 10
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No
  Access Denied Message  : System Default

                 Client Client Logoff    Re-Auth   Unauth  Auth    Cntrl
  Port   Enabled Limit  Moves  Period    Period    VLAN ID VLAN ID Dir
  ------ ------- ------ ------ --------- --------- ------- ------- -----
  18     Yes     5      No     300       0         99      0       both
```

Comware5

```
[Comware5]radius scheme <radius-auth>

[Comware5-radius-radius-auth]primary authentication 10.0.100.111 1812

[Comware5-radius-radius-auth]primary accounting 10.0.100.111 1813

[Comware5-radius-radius-auth]key authentication password
```

```
[Comware5-radius-radius-auth]user-name-format without-domain

[Comware5-radius-radius-auth]server-type extended


[Comware5]domain web-auth
New Domain added.

[Comware5-isp-web-auth]?
Isp view commands:

  access-limit             Specify access limit of domain
  accounting               Specify accounting scheme
  authentication           Specify authentication scheme
  authorization            Specify authorization scheme
  authorization-attribute  Specify authorization attributes of domain
  cfd                      Connectivity fault detection (IEEE 802.1ag)
  display                  Display current system information
  dscp                     Specify a DSCP value for user packets of this domain
  idle-cut                 Specify idle-cut attribute of domain
  mtracert                 Trace route to multicast source
  ping                     Ping function
  quit                     Exit from current command view
  return                   Exit to User View
  save                     Save current configuration
  self-service-url         Specify self-service URL(Uniform Resource Locator)
                           of domain
  state                    Specify state of domain
  tracert                  Trace route function
  undo                     Cancel current setting

[Comware5-isp-web-auth]authentication ?
  default     Specify default AAA configuration
  lan-access  Specify lan-access AAA configuration
  login       Specify login AAA configuration
  portal      Specify portal AAA configuration
  super       Specify super AAA configuration

[Comware5-isp-web-auth]authentication portal ?
  local          Specify local scheme
  none           Specify none scheme
  radius-scheme  Specify RADIUS scheme

[Comware5-isp-web-auth]authentication portal radius-scheme ?
  STRING<1-32>  Scheme name

[Comware5-isp-web-auth]authentication portal radius-scheme radius-auth ?
  local  Specify local scheme
  <cr>

[Comware5-isp-web-auth]authentication portal radius-scheme radius-auth


[Comware5-isp-web-auth]authorization ?
  command     Specify command AAA configuration
  default     Specify default AAA configuration
  lan-access  Specify lan-access AAA configuration
  login       Specify login AAA configuration
  portal      Specify portal AAA configuration

[Comware5-isp-web-auth]authorization portal ?
  local          Specify local scheme
  none           Specify none scheme
```

```
  radius-scheme  Specify RADIUS scheme

[Comware5-isp-web-auth]authorization portal radius-scheme ?
  STRING<1-32>  Scheme name

[Comware5-isp-web-auth]authorization portal radius-scheme radius-auth ?
  local  Specify local scheme
  <cr>

[Comware5-isp-web-auth]authorization portal radius-scheme radius-auth


[Comware5-isp-web-auth]accounting ?
  command     Specify command AAA configuration
  default     Specify default AAA configuration
  lan-access  Specify lan-access AAA configuration
  login       Specify login AAA configuration
  optional    Optional accounting mode
  portal      Specify portal AAA configuration

[Comware5-isp-web-auth]accounting portal ?
  local          Specify local scheme
  none           Specify none scheme
  radius-scheme  Specify RADIUS scheme

[Comware5-isp-web-auth]accounting portal radius-scheme ?
  STRING<1-32>  Scheme name

[Comware5-isp-web-auth]accounting portal radius-scheme radius-auth ?
  local  Specify local scheme
  <cr>

[Comware5-isp-web-auth]accounting portal radius-scheme radius-auth


[Comware5] interface LoopBack 12

[Comware5-LoopBack12]ip address 1.1.1.1 255.255.255.255


[Comware5]portal ?
  delete-user   Delete user
  free-rule     Configure free rule
  local-server  Configure local portal server
  max-user      Specify the maximum number of online users
  move-mode     Specify port admission mode for layer 2 portal user moving from
                one access port to another
  redirect-url  Specify the URL address of the page to be pushed to user after
                Portal authentication success
  server        Configure portal server
  web-proxy     Specify Web proxy information of portal client

[Comware5]portal local-server ?
  http   Enable HTTP protocol
  https  Enable HTTPS protocol
  ip     Specify listening IP address of local portal server

[Comware5]portal local-server ip ?
  X.X.X.X  Listening IP address

[Comware5]portal local-server ip 1.1.1.1 ?
  <cr>
```

```
[Comware5]portal local-server ip 1.1.1.1

[Comware5]portal local-server http


[Comware5]interface  g1/0/18

[Comware5-GigabitEthernet1/0/18]port link-type hybrid

[Comware5-GigabitEthernet1/0/18]mac-vlan enable

[Comware5-GigabitEthernet1/0/18]portal ?
  auth-fail       Specify a VLAN for clients failing the portal authentication
                  on the port
  domain          Configure domain
  local-server    Configure local portal server
  offline-detect  Specify offline detect timer configuration

[Comware5-GigabitEthernet1/0/18]portal local-server enable ?
  <cr>

[Comware5-GigabitEthernet1/0/18]portal local-server ?
  enable  Enable local portal server

[Comware5-GigabitEthernet1/0/18]portal local-server enable

[Comware5-GigabitEthernet1/0/18]portal domain ?
  STRING<1-24>  Domain name
  ipv6          Specify the domain for IPv6 portal authentication

[Comware5-GigabitEthernet1/0/18]portal domain web-auth

[Comware5-GigabitEthernet1/0/18]portal auth-fail vlan 99

[Comware5-GigabitEthernet1/0/18]stp edged-port enable
 Warning: Edge port should only be connected to terminal. It will cause temporary loops if
port GigabitEthernet1/0/18 is connected to bridges. Please use it carefully!


[Comware5]display portal ?
  acl           Display portal ACL(s)
  connection    Display connection statistics
  free-rule     Display free rule
  interface     Display interface
  local-server  Display local portal server
  server        Display portal server
  tcp-cheat     Display TCP-cheat statistics
  user          Display portal user(s)

[Comware5]display portal user ?
  all        All
  interface  Specify interface

[Comware5]display portal user all
Index:3
 State:ONLINE
 SubState:NONE
 ACL:NONE
 Work-mode:stand-alone
 VPN instance:NONE
 MAC              IP                Vlan   Interface
 ---------------------------------------------------------------------------
 705a-b6e8-6783   10.1.220.102      220    GigabitEthernet1/0/18
```

```
 Total 1 user(s) matched, 1 listed.


[Comware5]display connection ?
  access-type  Connection by access mode
  domain       Connection by domain name
  interface    Connection by interface
  ip           Connection by IP address
  mac          Connection by MAC address
  slot         Specify slot number
  ucibindex    Connection by UCIB index
  user-name    Connection by user name
  vlan         Connection by VLAN-ID
  |            Matching output
  <cr>

[Comware5]display connection access-type ?
  dot1x               8021x access mode
  mac-authentication  MAC-authentication access mode
  portal              PORTAL access mode

[Comware5]display connection access-type portal
Slot:  1
Index=3   , Username=user1@web-auth
 IP=10.1.220.102
 IPv6=N/A
 MAC=705a-b6e8-6783


[Comware5]display connection ucibindex 3
Slot:  1
Index=3   , Username=user1@web-auth
MAC=705a-b6e8-6783
IP=10.1.220.102
IPv6=N/A
Access=PORTAL  ,AuthMethod=PAP
Port Type=Ethernet,Port Name=GigabitEthernet1/0/18
Initial VLAN=1, Authorization VLAN=220
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
SessionTimeout=N/A, Terminate-Action=N/A
Start=2015-05-19 15:39:14 ,Current=2015-05-19 15:43:16 ,Online=00h04m03s
 Total 1 connection matched.


[Comware5]display portal connection statistics all
---------------Interface: GigabitEthernet1/0/18-----------------------
 User state statistics:
 State-Name                User-Num
 VOID                      0
 DISCOVERED                0
 WAIT_AUTHEN_ACK           0
 WAIT_EAP_ACK              0
 WAIT_AUTHOR_ACK           0
 WAIT_LOGIN_ACK            0
 WAIT_ACL_ACK              0
 WAIT_NEW_IP               0
 WAIT_USERIPCHANGE_ACK     0
 ONLINE                    1
 WAIT_LOGOUT_ACK           0
 WAIT_LEAVING_ACK          0
```

```
Message statistics:
Msg-Name                    Total          Err            Discard
MSG_AUTHEN_ACK              1              0              0
MSG_CONTINUE_ACK            0              0              0
MSG_AUTHOR_ACK              1              0              0
MSG_LOGIN_ACK               1              0              0
MSG_LOGOUT_ACK              0              0              0
MSG_LEAVING_ACK             0              0              0
MSG_CUT_REQ                 0              0              0
MSG_AUTH_REQ                1              0              0
MSG_LOGIN_REQ               1              0              0
MSG_LOGOUT_REQ              0              0              0
MSG_LEAVING_REQ             0              0              0
MSG_ARPPKT                  0              0              0
MSG_PORT_REMOVE             0              0              0
MSG_VLAN_REMOVE             0              0              0
MSG_IF_REMOVE               0              0              0
MSG_IF_SHUT                 0              0              0
MSG_IF_DISPORTAL            0              0              0
MSG_IF_UP                   0              0              0
MSG_ACL_RESULT              0              0              0
MSG_AAACUTBKREQ             0              0              0
MSG_CUT_BY_USERINDEX        0              0              0
MSG_CUT_L3IF                0              0              0
MSG_ALL_REMOVE              0              0              0
MSG_IFIPADDR_CHANGE         0              0              0
MSG_SOCKET_CHANGE           0              0              0
MSG_NOTIFY                  0              0              0
MSG_SETPOLICY               0              0              0
MSG_SETPOLICY_RESULT        0              0              0
```

Comware7

Note: Comware7 does not support local web portal server functions.

Cisco

(note - requires special configuration on the RADIUS server)

```
Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key password

Cisco(config)#radius-server attribute ?
  11            Filter-Id attribute configuration
  188           Num-In-Multilink attribute configuration
  218           Address-Pool attribute
  25            Class attribute
  30            DNIS attribute
  31            Calling Station ID
  32            NAS-Identifier attribute
  4             NAS IP address attribute
  44            Acct-Session-Id attribute
  55            Event-Timestamp attribute
  6             Service-Type attribute
  61            NAS-Port-Type attribute configuration
  69            Tunnel-Password attribute
  77            Connect-Info attribute
  8             Framed IP address attribute
  95            NAS IPv6 address attribute
  list          List of Attribute Types
  nas-port      NAS-Port attribute configuration
  nas-port-id   Nas-Port-Id attribute configuration

Cisco(config)#radius-server attribute 8 ?
```

```
  include-in-access-req  Send attribute 8 in access-req packet

Cisco(config)#radius-server attribute 8 include-in-access-req ?
  <cr>

Cisco(config)#radius-server attribute 8 include-in-access-req


Cisco(config)#radius-server vsa send ?
  accounting      Send in accounting requests
  authentication  Send in access requests
  cisco-nas-port  Send cisco-nas-port VSA(2)
  <cr>

Cisco(config)#radius-server vsa send authentication ?
  3gpp2  Send 3GPP2 VSAs in accounting requests
  <cr>

Cisco(config)#radius-server vsa send authentication


Cisco(config)#aaa new-model

Cisco(config)#aaa ?
  accounting       Accounting configurations parameters.
  attribute        AAA attribute definitions
  authentication   Authentication configurations parameters.
  authorization    Authorization configurations parameters.
  cache            AAA cache definitions
  configuration    Authorization configuration parameters.
  dnis             Associate certain AAA parameters to a specific DNIS number
  group            AAA group definitions
  local            AAA Local Authen/Authz Method Lists
  local            AAA Local method options
  max-sessions     Adjust initial hash size for estimated max sessions
  memory           AAA memory parameters
  nas              NAS specific configuration
  new-model        Enable NEW access control commands and functions.(Disables
                   OLD commands.)
  pod              POD processing
  policy           AAA policy parameters
  server           Local AAA server
  service-profile  Service-Profile parameters
  session-id       AAA Session ID
  traceback        Traceback recording
  user             AAA user definitions

Cisco(config)#aaa authentication ?
  arap             Set authentication lists for arap.
  attempts         Set the maximum number of authentication attempts
  banner           Message to use when starting login/authentication.
  dot1x            Set authentication lists for IEEE 802.1x.
  enable           Set authentication list for enable.
  eou              Set authentication lists for EAPoUDP
  fail-message     Message to use for failed login/authentication.
  login            Set authentication lists for logins.
  password-prompt  Text to use when prompting for a password
  ppp              Set authentication lists for ppp.
  sgbp             Set authentication lists for sgbp.
  suppress         Do not send access request for a specific type of user.
  username-prompt  Text to use when prompting for a username

Cisco(config)#aaa authentication login ?
```

```
  WORD     Named authentication list (max 31 characters, longer will be
           rejected).
  default  The default authentication list.

Cisco(config)#aaa authentication login default ?
  cache          Use Cached-group
  enable         Use enable password for authentication.
  group          Use Server-group
  krb5           Use Kerberos 5 authentication.
  krb5-telnet    Allow logins only if already authenticated via Kerberos V
                 Telnet.
  line           Use line password for authentication.
  local          Use local username authentication.
  local-case     Use case-sensitive local username authentication.
  none           NO authentication.
  passwd-expiry  enable the login list to provide password aging support

Cisco(config)#aaa authentication login default group ?
  WORD     Server-group name
  ldap     Use list of all LDAP hosts.
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.

Cisco(config)#aaa authentication login default group radius ?
  cache       Use Cached-group
  enable      Use enable password for authentication.
  group       Use Server-group
  krb5        Use Kerberos 5 authentication.
  line        Use line password for authentication.
  local       Use local username authentication.
  local-case  Use case-sensitive local username authentication.
  none        NO authentication.
  <cr>

Cisco(config)#aaa authentication login default group radius

Cisco(config)#aaa authorization ?
  auth-proxy           For Authentication Proxy Services
  cache                For AAA cache configuration
  commands             For exec (shell) commands.
  config-commands      For configuration mode commands.
  configuration        For downloading configurations from AAA server
  console              For enabling console authorization
  credential-download  For downloading EAP credential from Local/RADIUS/LDAP
  exec                 For starting an exec (shell).
  multicast            For downloading Multicast configurations from an AAA
                       server
  network              For network services. (PPP, SLIP, ARAP)
  policy-if            For diameter policy interface application.
  prepaid              For diameter prepaid services.
  radius-proxy         For proxying radius packets
  reverse-access       For reverse access connections
  subscriber-service   For iEdge subscriber services (VPDN etc)
  template             Enable template authorization

Cisco(config)#aaa authorization auth-proxy ?
  default  The default authorization list.

Cisco(config)#aaa authorization auth-proxy default ?
  cache  Use Cached-group
  group  Use server-group.
  local  Use local database.
```

```
Cisco(config)#aaa authorization auth-proxy default group ?
  WORD     Server-group name
  ldap     Use list of all LDAP hosts.
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.

Cisco(config)#aaa authorization auth-proxy default group radius ?
  cache  Use Cached-group
  group  Use server-group.
  local  Use local database.
  <cr>

Cisco(config)#aaa authorization auth-proxy default group radius


Cisco(config)#ip device tracking


Cisco(config)#ip admission ?
  absolute-timer      Absolute Timeout in minutes
  auth-proxy-audit    Authentication Proxy Auditing
  auth-proxy-banner   Authentication Proxy Banner
  http                Configure maximum HTTP process
  inactivity-timer    Inactivity Timeout in minutes
  init-state-time     Init State Timeout
  max-login-attempts  Max Login attempts per user
  name                Specify an Authentication Proxy Rule
  proxy               Authentication proxy protocol
  ratelimit           Session Ratelimit
  service-policy      Service Policy
  source-interface    IP Admission Source Interface
  watch-list          Watch-list

Cisco(config)#ip admission name ?
  WORD  Name of Authentication Rule

Cisco(config)#ip admission name web-auth-rule1 ?
  consent  Consent page parameters
  eapoudp  EAPoUDP Validate Posture Credentials
  proxy    Authentication Proxy Protocol

Cisco(config)#ip admission name web-auth-rule1 proxy ?
  http  HTTP Protocol

Cisco(config)#ip admission name web-auth-rule1 proxy http ?
  absolute-timer   Absolute Timeout in minutes
  inactivity-time  Inactivity timeout in minutes
  list             Specify an access-list to apply to authentication proxy
  service-policy   Service Policy
  <cr>

Cisco(config)#ip admission name web-auth-rule1 proxy http


Cisco(config)#ip admission auth-proxy-banner ?
  file  Specify the banner file for HTTP
  http  HTTP Protocol Banner

Cisco(config)#ip admission auth-proxy-banner http ?
  LINE  c banner-text c, where 'c' is a delimiting character
  <cr>

Cisco(config)#ip admission auth-proxy-banner http
```

```
Cisco(config)#ip access-list extended web-auth-policy1

Cisco(config-ext-nacl)#permit udp any any

Cisco(config-ext-nacl)#permit tcp any any eq www

Cisco(config-ext-nacl)#deny ip any any


Cisco(config)#fallback ?
  profile  Create a Fallback profile

Cisco(config)#fallback profile ?
  WORD  Specify a policy name

Cisco(config)#fallback profile fallback1

Cisco(config-fallback-profile)#ip access-group web-auth-policy1 in

Cisco(config-fallback-profile)#ip admission web-auth-rule1


Cisco(config)#interface g1/0/18

Cisco(config-if)#switchport mode access

Cisco(config-if)#switchport access vlan 220

Cisco(config-if)#dot1x ?
  authenticator   Configure authenticator parameters
  credentials     Credentials profile configuration
  default         Configure Dot1x with default values for this port
  max-reauth-req  Max No. of Reauthentication Attempts
  max-req         Max No. of Retries
  max-start       Max No. of EAPOL-Start requests
  pae             Set 802.1x interface pae type
  supplicant      Configure supplicant parameters
  timeout         Various Timeouts

Cisco(config-if)#dot1x pae ?
  authenticator  Set pae type as Authenticator
  both           Set pae type as both Supplicant and Authenticator
  supplicant     Set pae type as Supplicant

Cisco(config-if)#dot1x pae authenticator ?
  <cr>

Cisco(config-if)#dot1x pae authenticator

Cisco(config-if)#authentication ?
  control-direction  Set the control-direction on the interface
  event              Set action for authentication events
  fallback           Enable the Webauth fallback mechanism
  host-mode          Set the Host mode for authentication on this interface
  linksec            Configure link security parameters
  open               Enable or Disable open access on this port
  order              Add an authentication method to the order list
  periodic           Enable or Disable Reauthentication for this port
  port-control       Set the port-control value
  priority           Add an authentication method to the priority list
  timer              Set authentication timer values
```

```
  violation          Configure action to take on security violations

Cisco(config-if)#authentication fallback fallback1

Cisco(config-if)#authentication order webauth

Cisco(config-if)#authentication port-control auto

Cisco(config-if)#ip access-group web-auth-policy1 in

Cisco(config-if)#ip admission web-auth-rule1


Cisco#show ip admission cache
Authentication Proxy Cache
Total Sessions: 1 Init Sessions: 0
 Client IP 10.1.220.102 Port 49647, timeout 60, state ESTAB

Cisco#show authentication interface g1/0/18

Client list:
Interface  MAC Address     Method   Domain   Status         Session ID
  Gi1/0/18   705a.b6e8.6783  webauth  DATA     Authz Success  0A00002900000007006B16FC

Available methods list:
  Handle  Priority  Name
    3        0      dot1x
    1        2      webauth
Runnable methods list:
  Handle  Priority  Name
    1        0      webauth
```

Chapter 36 Port Mirroring or Port Span

This chapter compares the commands used to configure local mirroring and remote mirroring.

Traffic mirroring allows you to mirror (send a copy of) network traffic received or transmitted on a switch interface to a local or remote destination, such as a traffic analyzer or intrusion detection system (IDS).

Traffic mirroring provides the following benefits:

- It allows you to monitor the traffic flow on specific source interfaces.
- It helps in analyzing and debugging problems in network operation resulting from a misbehaving network or an individual client. The mirroring of selected traffic to an external device makes it easier to diagnose a network problem from a centralized location in a topology spread across a campus.
- It supports remote mirroring to simultaneously mirror switch traffic on one or more interfaces to multiple remote destinations.

a) Local Mirror or SPAN

ArubaOS-Switch	Comware	Cisco
(Note: ArubaOS-Switch manual indicates to configure destination then source)	(Note: Comware manual indicates to configure source then destination)	(Note: Cisco manual indicates to configure source then destination)
	`[Comware]mirroring-group 1 local`	
	`[Comware]mirroring-group 1 mirroring-port g1/0/6 both`	`Cisco(config)#monitor session 1 source interface g1/0/6 both`
`ArubaOS-Switch(config)# mirror 1 port 4`	`[Comware]mirroring-group 1 monitor-port g1/0/4`	`Cisco(config)# monitor session 1 destination interface g1/0/4 encapsulation replicate`
`ArubaOS-Switch(config)# interface 11 monitor all both mirror 1`		
`ArubaOS-Switch# show monitor`	`[Comware]display mirroring-group all`	`Cisco#show monitor`
`ArubaOS-Switch# show monitor 1`	`[Comware]display mirroring-group 1`	`Cisco#show monitor session 1`
		`Cisco#show monitor session 1 detail`

ArubaOS-Switch

(Note: ArubaOS-Switch manual indicates to configure destination then source)

```
ArubaOS-Switch(config)# mirror ?
 endpoint              Remote mirroring destination configuration.
 <1-4>                 Mirror destination number.

ArubaOS-Switch(config)# mirror 1 ?
```

```
 name                   Mirroring destination name string.
 port                   Mirroring destination monitoring port.
 remote                 Remote mirroring destination configuration.

ArubaOS-Switch(config)# mirror 1 port ?
 [ethernet] PORT-NUM   Enter a port name for the 'port' command/parameter.

ArubaOS-Switch(config)# mirror 1 port 4 ?
 <cr>

ArubaOS-Switch(config)# mirror 1 port 4


ArubaOS-Switch(config)# interface 11 monitor ?
 all                    Monitor all traffic.
 <cr>

ArubaOS-Switch(config)# interface 11 monitor all ?
 in                     Monitor all inbound traffic
 out                    Monitor all outbound traffic
 both                   Monitor all inbound and outbound traffic

ArubaOS-Switch(config)# interface 11 monitor all both ?
 mirror                 Mirror destination.

ArubaOS-Switch(config)# interface 11 monitor all both mirror ?
 <1-4>                  Mirror destination number.

ArubaOS-Switch(config)# interface 11 monitor all both mirror 1 ?
 no-tag-added           Don't add VLAN tag for this untagged-port
 <1-4>                  Mirror destination number.
 <cr>

ArubaOS-Switch(config)# interface 11 monitor all both mirror 1


ArubaOS-Switch# show monitor ?
 endpoint               Remote mirroring destination configuration.
 <1-4>                  Mirror destination number.
 <cr>

ArubaOS-Switch# show monitor
There are no Remote Mirroring endpoints currently assigned.

Network Monitoring

   Sessions  Status       Type    Sources  Mirror-Policy
   --------  -----------  -----   -------  -------------
   1         active        port   1
   2         not defined
   3         not defined
   4         not defined


ArubaOS-Switch# show monitor 1
Network Monitoring

   Session: 1    Session Name:
      Mirror Destination:  4     (Port)

      Monitoring Sources  Direction Truncation Mirror Policy
      ------------------  --------- ---------- -------------
      Port: 11            Both       No         -
```

Comware

(Note: Comware manual indicates to configure source then destination)

```
[Comware]mirroring-group ?
  INTEGER<1-4>  Mirroring group number

[Comware]mirroring-group 1 ?
  local               Local mirroring group
  mirroring-port      Specify mirroring port
  monitor-egress      Specify monitor-egress port
  monitor-port        Specify monitor port
  reflector-port      Specify reflector port
  remote-destination  Remote destination mirroring group
  remote-probe        Specify remote probe VLAN
  remote-source       Remote source mirroring group

[Comware]mirroring-group 1 local ?
  <cr>

[Comware]mirroring-group 1 local


[Comware]mirroring-group 1 mirroring-port ?
  GigabitEthernet  GigabitEthernet interface

[Comware]mirroring-group 1 mirroring-port g1/0/6 ?
  GigabitEthernet  GigabitEthernet interface
  both             Monitor the inbound and outbound packets
  inbound          Monitor the inbound packets
  outbound         Monitor the outbound packets
  to               Range of interfaces

[Comware]mirroring-group 1 mirroring-port g1/0/6 both ?
  <cr>

[Comware]mirroring-group 1 mirroring-port g1/0/6 both


[Comware]mirroring-group 1 monitor-port ?
  Bridge-Aggregation  Bridge-Aggregation interface
  GigabitEthernet     GigabitEthernet interface

[Comware]mirroring-group 1 monitor-port g1/0/4 ?
  <cr>

[Comware]mirroring-group 1 monitor-port g1/0/4


[Comware]display mirroring-group ?
  INTEGER<1-4>        Mirroring group number
  all                 all mirroring group
  local               Local mirroring group
  remote-destination  Remote destination mirroring group
  remote-source       Remote source mirroring group

[Comware]dis mirroring-group all
mirroring-group 1:
    type: local
    status: active
    mirroring port:
        GigabitEthernet1/0/6  both
```

```
    monitor port: GigabitEthernet1/0/4


[Comware]display mirroring-group 1
mirroring-group 1:
    type: local
    status: active
    mirroring port:
        GigabitEthernet1/0/6  both
    monitor port: GigabitEthernet1/0/4
```

Cisco

(Note: Cisco manual indicates to configure source then destination)

```
Cisco(config)#monitor ?

  event-trace  Tracing of system events
  session      Configure a SPAN session

Cisco(config)#monitor session ?

  <1-66>  SPAN session number

Cisco(config)#monitor session 1 ?

  destination  SPAN destination interface or VLAN
  filter       SPAN filter VLAN
  source       SPAN source interface, VLAN

Cisco(config)#monitor session 1 source ?

  interface  SPAN source interface
  remote     SPAN source Remote
  vlan       SPAN source VLAN

Cisco(config)#monitor session 1 source interface g1/0/6 ?
  ,     Specify another range of interfaces
  -     Specify a range of interfaces
  both  Monitor received and transmitted traffic
  rx    Monitor received traffic only
  tx    Monitor transmitted traffic only

  <cr>

Cisco(config)#monitor session 1 source interface g1/0/6 both ?
  <cr>

Cisco(config)#monitor session 1 source interface g1/0/6 both


Cisco(config)#monitor session 1 destination ?

  interface  SPAN destination interface
  remote     SPAN destination Remote


Cisco(config)#monitor session 1 destination interface g1/0/4 ?
  ,              Specify another range of interfaces
  -              Specify a range of interfaces
  encapsulation  Set encapsulation for destination interface
  ingress        Enable ingress traffic forwarding
```

```
  <cr>


Cisco(config)#monitor session 1 destination interface g1/0/4 encapsulation ?

  dot1q      interface uses only dot1q encapsulation
  isl        interface uses only isl encapsulation
  replicate  interface replicates source encapsulation

Cisco(config)#monitor session 1 destination interface g1/0/4 encapsulation replicate ?
  ingress  Enable ingress traffic forwarding

  <cr>

Cisco(config)#monitor session 1 destination interface g1/0/4 encapsulation replicate


Cisco#show monitor ?

  capture      Packet Capture Information
  detail       Detailed SPAN information
  event-trace  Trace information
  session      SPAN session
  |            Output modifiers

  <cr>

Cisco#show monitor

Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Gi1/0/6
Destination Ports      : Gi1/0/4
    Encapsulation      : Replicate
          Ingress      : Disabled


Cisco#show monitor session 1

Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Gi1/0/6
Destination Ports      : Gi1/0/4
    Encapsulation      : Replicate
          Ingress      : Disabled


Cisco#show monitor session 1 detail

Session 1
---------

Type                   : Local Session
Description            : -
Source Ports           :
    RX Only            : None
    TX Only            : None
    Both               : Gi1/0/6
Source VLANs           :
```

```
    RX Only             : None
    TX Only             : None
    Both                : None
Source RSPAN VLAN       : None
Destination Ports       : Gi1/0/4
    Encapsulation       : Replicate
          Ingress       : Disabled
Filter VLANs            : None
Dest RSPAN VLAN         : None
IP Access-group         : None
MAC Access-group        : None
IPv6 Access-group       : None
```

b) Remote Mirror or RSPAN

With remote mirroring on ArubaOS-Switch, mirrored traffic can traverse Layer 3 networks. With remote mirroring on Comware and Cisco, mirrored traffic traverses the same Layer 2 network (subnet).

ArubaOS-Switch	Comware	Cisco
(switch where analyzer is connected)	(switch with traffic of interest)	(switch with traffic of interest)
ArubaOS-Switch(config)# mirror endpoint ip 10.0.222.254 7922 10.0.111.21 port 4	[Comware2]mirroring-group 1 remote-source	Cisco2(config)#vlan 950
	[Comware2]mirroring-group 1 mirroring-port g1/0/1 both	Cisco2(config-vlan)#remote-span
	[Comware2]interface g1/0/1	Cisco2(config)#interface f1/0/6
	[Comware2-GigabitEthernet1/0/1] mirroring-group 1 mirroring-port both	Cisco2(config-if)#switchport trunk encapsulation dot1q Cisco2(config-if)#switchport trunk allowed vlan 950 Cisco2(config-if)#switchport mode trunk Cisco2(config-if)#switchport nonegotiate
	[Comware2]mirroring-group 1 monitor-egress g1/0/6	Cisco(config)# monitor session 1 source interface f1/0/1
	[Comware]vlan 960 [Comware2-vlan960]quit	Cisco2(config)# monitor session 1 destination remote vlan 950
	[Comware2]interface g1/0/6	
	[Comware2-GigabitEthernet1/0/6]port link-type trunk [Comware2-GigabitEthernet1/0/6]port trunk permit vlan 960	
	[Comware2]mirroring-group 1 remote-probe vlan 960	
ArubaOS-Switch# show monitor	[Comware2]display mirroring-group 1	Cisco2#show monitor
ArubaOS-Switch# show monitor endpoint		Cisco2#show monitor session 1 detail
(switch with traffic of interest)	(switch where analyzer is connected)	(switch where analyzer is connected)
ArubaOS-Switch2(config)# mirror endpoint ip 10.0.222.254 7922 10.0.111.21	[Comware]vlan 960 [Comware-vlan960]quit	Cisco(config)#vlan 950
ArubaOS-Switch2(config)# interface 1 monitor all both mirror 1	[Comware]mirroring-group 1 remote-destination	Cisco(config-vlan)#remote-span
	[Comware]mirroring-group 1 monitor-port g1/0/4	Cisco(config)#interface g1/0/12

	[Comware]mirroring-group 1 remote-probe vlan 960	Cisco(config-if)#switchport trunk encapsulation dot1q Cisco(config-if)#switchport trunk allowed vlan 950 Cisco(config-if)#switchport mode trunk Cisco(config-if)#switchport nonegotiate
	[Comware]interface g1/0/12	Cisco(config)#monitor session 1 source remote vlan 950
	[Comware-GigabitEthernet1/0/12]port link-type trunk [Comware-GigabitEthernet1/0/12]port trunk permit vlan 960	Cisco(config)#monitor session 1 destination interface g1/0/4 encapsulation replicate
ArubaOS-Switch2# show monitor 1	[Comware]display mirroring-group 1	Cisco#show monitor
		Cisco#show monitor session 1 detail

ArubaOS-Switch

(switch where analyzer is connected)

```
ArubaOS-Switch(config)# mirror endpoint
 ip                     Remote mirroring destination configuration.

ArubaOS-Switch(config)# mirror endpoint ip
 IP-ADDR                Enter an IP address.

ArubaOS-Switch(config)# mirror endpoint ip 10.0.222.254
 <1-65535>              Remote mirroring UDP encapsulation port.

ArubaOS-Switch(config)# mirror endpoint ip 10.0.222.254 7922
 IP-ADDR                Remote mirroring UDP encapsulation destination ip addr.

ArubaOS-Switch(config)# mirror endpoint ip 10.0.222.254 7922 10.0.111.21
 port                   Remote mirroring destination port.

ArubaOS-Switch(config)# mirror endpoint ip 10.0.222.254 7922 10.0.111.21 port
 [ethernet] PORT-NUM    Enter a port name.

ArubaOS-Switch(config)# mirror endpoint ip 10.0.222.254 7922 10.0.111.21 port 4


ArubaOS-Switch# show monitor
Mirroring is currently disabled.

Remote Mirroring - Remote Endpoints

 Type  UDP Source Addr  UDP port  UDP Dest Addr    Dest Port
 ----  ---------------  --------  ---------------  ---------
 IPv4  10.0.222.254     7922      10.0.111.21      4
```

```
ArubaOS-Switch# show monitor endpoint
Remote Mirroring - Remote Endpoints

 Type  UDP Source Addr  UDP port  UDP Dest Addr    Dest Port
 ----  ---------------  --------  ---------------  ---------
 IPv4  10.0.222.254     7922      10.0.111.21      4
```

(switch with traffic of interest)

```
ArubaOS-Switch2(config)# mirror endpoint ip 10.0.222.254 7922 10.0.111.21
Caution: Please configure destination switch first.
         Do you want to continue [y/n]?  y

ArubaOS-Switch2(config)# interface 1 monitor all both mirror 1


ArubaOS-Switch2# show monitor 1
Network Monitoring

   Session: 1    Session Name:
      Mirror Destination:  IPv4
         UDP Source Addr  UDP port  UDP Dest Addr    Status
         ---------------  --------  ---------------  --------
         10.0.222.254     7922      10.0.111.21      active

      Monitoring Sources  Direction Truncation Mirror Policy
      ------------------  --------- ---------- -------------
      Port: 1             Both       No         -
```

Comware

(switch with traffic of interest)

```
[Comware2]mirroring-group ?
  INTEGER<1-4>  Mirroring group number

[Comware2]mirroring-group 1 ?
  local               Local mirroring group
  mirroring-port      Specify mirroring port
  monitor-egress      Specify monitor-egress port
  monitor-port        Specify monitor port
  reflector-port      Specify reflector port
  remote-destination  Remote destination mirroring group
  remote-probe        Specify remote probe VLAN
  remote-source       Remote source mirroring group

[Comware2]mirroring-group 1 remote-source ?
  <cr>

[Comware2]mirroring-group 1 remote-source


[Comware2]mirroring-group 1 mirroring-port g1/0/1 ?
  GigabitEthernet  GigabitEthernet interface
  both             Monitor the inbound and outbound packets
  inbound          Monitor the inbound packets
  outbound         Monitor the outbound packets
  to               Range of interfaces
```

```
[Comware2]mirroring-group 1 mirroring-port g1/0/1 both

[Comware2]interface g1/0/1

[Comware2-GigabitEthernet1/0/1]mirroring-group 1 mirroring-port both

[Comware2-GigabitEthernet1/0/1]quit

[Comware2]mirroring-group 1 monitor-egress g1/0/6

[Comware2]vlan 960

[Comware2-vlan960]quit

[Comware2]interface g1/0/6

[Comware2-GigabitEthernet1/0/6]port link-type trunk

[Comware2-GigabitEthernet1/0/6]port trunk permit vlan 960

[Comware2-GigabitEthernet1/0/6]quit

[Comware2]mirroring-group 1 remote-probe vlan 960

[Comware2]display mirroring-group 1
mirroring-group 1:
    type: remote-source
    status: active
    mirroring port:
        GigabitEthernet1/0/1  both
    reflector port:
    monitor egress port: GigabitEthernet1/0/6
    remote-probe VLAN: 960
```

(switch where analyzer is connected)

```
[Comware]vlan 960

[Comware-vlan960]quit

[Comware]mirroring-group 1 remote-destination

[Comware]mirroring-group 1 monitor-port g1/0/4

[Comware]mirroring-group 1 remote-probe vlan 960

[Comware]interface g1/0/12

[Comware-GigabitEthernet1/0/12]port link-type trunk
```

```
[Comware-GigabitEthernet1/0/12]port trunk permit vlan 960

[Comware-GigabitEthernet1/0/12]quit


[Comware]display mirroring-group 1
mirroring-group 1:
    type: remote-destination
    status: active
    monitor port: GigabitEthernet1/0/4
    remote-probe VLAN: 960
```

Cisco

(switch with traffic of interest)

```
Cisco2(config)#vlan 950

Cisco2(config-vlan)#remote-span


Cisco2(config)#interface f1/0/6

Cisco2(config-if)#switchport trunk encapsulation dot1q

Cisco2(config-if)#switchport trunk allowed vlan 950

Cisco2(config-if)#switchport mode trunk

Cisco2(config-if)#switchport nonegotiate


Cisco-2(config)#monitor session ?
  <1-66>  SPAN session number

Cisco-2(config)#monitor session 1 ?
  destination  SPAN destination interface or VLAN
  filter       SPAN filter VLAN
  source       SPAN source interface, VLAN

Cisco-2(config)#monitor session 1 source ?
  interface  SPAN source interface
  remote     SPAN source Remote
  vlan       SPAN source VLAN

Cisco-2(config)#monitor session 1 source interface f1/0/1 ?
  ,     Specify another range of interfaces
  -     Specify a range of interfaces
  both  Monitor received and transmitted traffic
  rx    Monitor received traffic only
  tx    Monitor transmitted traffic only
  <cr>

Cisco2(config)# monitor session 1 source interface f1/0/1 both

Cisco-2(config)#monitor session 1 destination ?
  interface  SPAN destination interface
  remote     SPAN destination Remote

Cisco-2(config)#monitor session 1 destination remote ?
  vlan  Remote SPAN destination RSPAN VLAN

Cisco2(config)# monitor session 1 destination remote vlan 950
```

```
Cisco-2#show monitor ?
  detail       Detailed SPAN information
  event-trace  Trace information
  session      SPAN session
  |            Output modifiers
  <cr>

Cisco2#show monitor
Session 1
---------
Type                   : Remote Source Session
Source Ports           :
    Both               : Fa1/0/1
Dest RSPAN VLAN        : 950


Cisco2#show monitor session 1 detail
Session 1
---------
Type                   : Remote Source Session
Description            : -
Source Ports           :
    RX Only            : None
    TX Only            : None
    Both               : Fa1/0/21
Source VLANs           :
    RX Only            : None
    TX Only            : None
    Both               : None
Source RSPAN VLAN      : None
Destination Ports      : None
Filter VLANs           : None
Dest RSPAN VLAN        : 950
IP Access-group        : None
MAC Access-group       : None
```

(switch where analyzer is connected)

```
Cisco(config)#vlan 950

Cisco(config-vlan)#remote-span

Cisco(config)#interface g1/0/12

Cisco(config-if)#switchport trunk encapsulation dot1q

Cisco(config-if)#switchport trunk allowed vlan 950

Cisco(config-if)#switchport mode trunk

Cisco(config-if)#switchport nonegotiate


Cisco(config)#monitor session 1 source ?
  interface  SPAN source interface
  remote     SPAN source Remote
```

```
  vlan       SPAN source VLAN

Cisco(config)#monitor session 1 source remote ?
  vlan  Remote SPAN source RSPAN VLAN

Cisco(config)#monitor session 1 source remote vlan 950 ?
  <cr>

Cisco(config)#monitor session 1 source remote vlan 950

Cisco(config)#monitor session 1 destination interface g1/0/4 encapsulation replicate


Cisco#show monitor
Session 1
---------
Type                   : Remote Destination Session
Source RSPAN VLAN      : 950
Destination Ports      : Gi1/0/4
    Encapsulation      : Replicate
          Ingress      : Disabled


Cisco#show monitor session 1 detail
Session 1
---------
Type                   : Remote Destination Session
Description            : -
Source Ports           :
    RX Only            : None
    TX Only            : None
    Both               : None
Source VLANs           :
    RX Only            : None
    TX Only            : None
    Both               : None
Source RSPAN VLAN      : 950
Destination Ports      : Gi1/0/4
    Encapsulation      : Replicate
          Ingress      : Disabled
Filter VLANs           : None
Dest RSPAN VLAN        : None
IP Access-group        : None
MAC Access-group       : None
IPv6 Access-group      : None
```

Chapter 37 Tunneled Node, Trust QoS, Clear Pass Intergration

Tunneled Node:

The Aruba tunneled node connects to one or more client devices at the edge of the network and then establishes a secure GRE tunnel to the controlling concentrator server. This approach allows the controller to support all the centralized security features, such as 802.1x authentication, captive-portal authentication, and stateful firewall. The Aruba tunneled node is required to handle only the physical connection to clients and support for its end of the GRE tunnel.

To support the wired concentrator, the controller must have a license to terminate access points (APs). No other configuration is required. To configure the Aruba tunneled node, you must specify the IP address of the controller and identify the ports that are to be used as active tunneled node ports. Tunnels are established between the controller and each active tunneled node port on the tunneled node. All tunneled node units must be running the same version of software. The tunneled node port can also be configured as a trunk port. This allows customers to have multiple clients on different VLANs that come through the trunk port instead of having clients on a single vlan.

Traffic moves through GRE tunnels between the active tunneled node ports and the controller or controllers. Policies are configured on a master server and enforced on the local controllers. The master and the controller can run on the same or different systems. The tunneled node can connect to the master, but it is not required.

On the controlling controller, you can assign the same policy to tunneled node user traffic as you would to any untrusted wired traffic. The profile specified by the **aaa authentication wired** command determines the initial role, which contains the policy. The VLAN setting on the concentrator port must match the VLAN that will be used for users at the local controller.

ArubaOS-Switch	Cisco
`ArubaOS-Switch(config)#tunneled-node-server backup-controller-ip 10.0.0.1`	`(Exact feature not supported)`
`ArubaOS-Switch(config)#tunneled-node-server enable`	
`ArubaOS-Switch(config)#tunneled-node-server controller-ip 10.0.0.1`	
`ArubaOS-Switch(config)#tunneled-node-server backup-controller-ip 10.0.0.1`	
`ArubaOS-Switch(config)#sh tunneled-node-server state`	
`ArubaOS-Switch(config)#sh tunneled-node-server state 2`	

ArubaOS-Switch(config)#sh tunneled-node-server statistics	
ArubaOS-Switch(config)#sh tunneled-node-server statistics 2	
ArubaOS-Switch(eth-1/1)# tunneled-node-server fallback-local-switching	

ArubaOS-Switch
ArubaOS-Switch(config)# tunneled-node-server keepalive <1-40> Configure the retry timeout for server requests. ArubaOS-Switch(eth-1/1)# tunneled-node-server fallback-local-swi Apply fallback option when communication with the controller fails. <cr> ArubaOS-Switch(eth-1/1)# tunneled-node-server fallback-local-switching

Trust QoS:

ArubaOS-Switch	Cisco
ArubaOS-Switch (eth-xy)#qos trust default	(Exact feature not supported)
ArubaOS-Switch (eth-xy)#qos trust dot1p	
ArubaOS-Switch (eth-xy)#qos trust dscp	
ArubaOS-Switch (eth-xy)#qos trust ip-prec	
ArubaOS-Switch (eth-xy)#qos trust none	
ArubaOS-Switch (eth-xy)#qos trust device aruba-ap	
ArubaOS-Switch (eth-xy)#qos trust device none	
ArubaOS-Switch (eth-xy)# qos trust <trust_mode>" help	
ArubaOS-Switch (eth-xy)#show qos trust	
ArubaOS-Switch (eth-xyz)# show qos trust device	
ArubaOS-Switch (eth-xyz)# show qos trust device <port>	

ArubaOS-Switch(config)#Qos dscp-map legacy	
ArubaOS-Switch(config)#Qos dscp-map default	

ArubaOS-Switch
ArubaOS-Switch(gigabitethernet "0/0/0")#qos trust ? aruba-device Trust DSCP/802.1p for Aruba-Device otherwise pass-through auto Trust DSCP for IP packets; 802.1p for non-IP packets disable Disable QoS trust (reset DSCP/802.1p to 0) dot1p Trust 802.1p dscp Trust DSCP pass-through Pass-through DSCP/802.1p

Clear Pass Integration:

As part of Aruba's Mobile First Platform Partner program, our ClearPass Exchange partners have developed security and operations features that integrate with our Aruba ClearPass Policy Management solution. These third-party IT systems – firewalls, MDM/EMM, and SIEM – leverage our REST based APIs, Syslog messaging, and our new Extensions repository to deliver end-to-end policy enforcement and visibility.

Aruba's ClearPass is a way for you to easily provide Wi-Fi network access to your visitors and employees. It securely provisions network access with context-aware policies that you can control and configure.

Envoy sends visitor information to ClearPass, which then provisions temporary Wi-Fi access credentials to your network. Upon sign-in, the visitor will receive an email (if you collect visitor email addresses) or text message (if you collect visitor phone numbers) with username and password information for Wi-Fi access.

Note: for this integration to work, you must collect either visitor email addresses or phone numbers at sign-in.

ArubaOS-Switch	Cisco
ArubaOS-Switch(config)#aaa authorization user-role enable	(Exact feature not supported)
ArubaOS-Switch(config)#aaa authorization user-role disable	
ArubaOS-Switch(config)#aaa authorization user-role initial-role USER_ROLE_1	
ArubaOS-Switch(config)#aaa authorization user-role name role1	

ArubaOS-Switch(user-role)# captive-portal-profile PROFILE_NAME	
ArubaOS-Switch(user-role)# no captive-portal-profile	
ArubaOS-Switch(user-role)# policy POLICY_NAME	
ArubaOS-Switch(user-role)# reauth-period 100	
ArubaOS-Switch(config)#show user-role	
ArubaOS-Switch(config)#show user-role ROLE_NAME	
ArubaOS-Switch(config)#show user-role ROLE_NAME detailed	
ArubaOS-Switch(policy-user) [no] [sequence-number] class ipv4|ipv6 <class-name> action deny	
ArubaOS-Switch(policy-user) [no] [sequence-number] class ipv4|ipv6 <class-name> action dscp <dscp-value>	
ArubaOS-Switch(policy-user) [no] [sequence-number] class ipv4|ipv6 <class-name> action ip-precedence <ip-precedence value>	
ArubaOS-Switch(config)#show captive-portal profile	
ArubaOS-Switch(config)#aaa port-access local-mac apply	

Chapter 38 HP 3800 Stacking / HP IRF / Cisco Switch Stacks

This chapter describes the commands used to configure stacking-related technologies on each of the three platforms.

These features allow multiple switches (within their respective platforms) to be configured to act as a single switch for both data and management. The feature capabilities are not interoperable between platforms/operating systems, but the basics of operations is similar.

In HP 3800 Stacking, one switch in the stack is designated as "Commander" and one switch is elected to be the "Standby." The other switches are designated "Member(s)." The Commander is responsible for the overall management of the stack. The Standby provides redundancy for the stack and takes over stack management operations should the Commander fail, or if an administrator forces a Commander failover. The Members are not part of the overall stack management; however, they must manage their local subsystems and ports to operate correctly as part of the stack. The Commander and Standby are also responsible for their own local subsystems and ports.

For features that you configure on specific switch ports in a stack, the configuration procedures are the same as for standalone switches, but the port designations for the ports in the stack are modified. Each port is identified by the stack member ID of its switch, followed by a slash and then the port number as it is shown on the switch. For example, for a switch with stack member ID 3, port 10 on that switch would be identified as port 3/10.

HP 3800 stacking is different from the stacking feature that is implemented on some other HPE Networking switches. HP 3800 Stacking requires a dedicated module installed in the HP 3800 switch. The other feature is implemented via the front-panel networking cables, uses a single IP address to manage the stack, and does not have the high bandwidth and redundancy features of HP 3800 stacking.

HP Intelligent Resilient Framework (IRF) technology creates an IRF fabric from multiple switches to provide data center class availability and scalability. When switches form an IRF fabric, they elect a master to manage the IRF fabric, and all other switches back up the master. When the master switch fails, the other switches automatically elect a new master from among them to take over.

Generally, IRF requires you to install expansion interface cards with dedicated 10-GbE ports in Comware capable switches.

For features that you configure on specific switch ports in an IRF fabric, the configuration procedures are the same as for standalone switches, but the port designations for the ports in the fabric are modified. Each port is identified by the member-id of its switch, followed by a slash and then the slot number of the

interface card, and then the port index as it is shown on the switch. For example, for a switch with member-id 3, slot number 0, and port index 10 on that switch would be identified as port 3/0/10.

Cisco Switch Stacks operate similar to HP 3800 Stacking. One of the switches controls the operation of the stack and is called the stack master. The stack master and the other switches in the stack are stack members. The stack master is the single point of management for the stack. All stack members are eligible stack masters. If the stack master becomes unavailable, the remaining stack members participate in electing a new stack master. One of the factors used to determine which switch is elected the stack master is the stack member priority value. The switch with the highest priority value becomes the stack master.

For features that you configure on specific switch ports in the switch stack, the configuration procedures are the same as for standalone switches, but the port designations for the ports in the stack are modified. Each port is identified by the member-id of its switch, followed by a slash and then the slot number of the interface card, and then the port index as it is shown on the switch. For example, for a switch with member-id 3, slot number 0, and port index 10 on that switch would be identified as port 3/0/10.

Cisco Switch Stacks require that the StackWise ports be interconnected between all the switches in the stack.

Cisco Switch Stacking is different from the clustering feature that is implemented on some other Cisco switches. Cisco Switch Stacking requires the dedicated StackWise ports. The clustering feature is implemented via the front-panel networking cables, uses a single IP address to manage the stcak, and does not have the high bandwidth and redundancy features of Switch Stacking.

Commands in this chapter are not "compared" as they are in other chapters, because the technologies are completely different designs. The commands listed are simply what is required to configure each individual platform.

ArubaOS-Switch

Note: In the default configuration, stacking is enabled on HP 3800 switches. However, if an HP 3800 switch is powered on and it does not have a Stacking Module installed, stacking is disabled. If a Stacking Module is subsequently installed in the switch, stacking must be enabled from the switch CLI (in the config context) by entering the following command:

```
HP Switch 3800(config)# stacking enable
```

The maximum number of HP 3800 switches allowed in the stack is sixteen.

Power on the first switch to be the Commander switch (with Stacking Module installed).

When the switch finishes booting, enter '`show stacking`' to view status:

```
HP Stack 3800# show stacking
Stack ID : NO ID - will merge upon connectivity
MAC Address : 1cc1de-4d48c0
Stack Topology : No Stack Formed
Stack Status : No Stack Formed
Uptime : 0d 0h 5m
Software Version : KA.15.03
Mbr
ID Mac Address Model Pri Status
--- ------------ ------------------------------------ --- -------
1 1cc1de-4d48c0 HP J9574A 3800-48G-PoE+-4SFP+ Switch 128 Commander


HP Switch 3800(config)# stacking set-stack

HP Switch 3800(config)# stacking member 1 priority 255
```

Connect the stacking cables to the module ports for the desired stacking topology.

Power on the second switch to be the Standby switch (with Stacking Module installed)

Power on the remaining switches and they will become Members of the stack when booted

When all of the switches are booted, enter the `show stacking` command to confirm that the stack is operating correctly:

```
HP Stack 3800# show stacking
Stack ID : 00031cc1-de4d48c0
MAC Address : 1cc1de-4d48c9
Stack Topology : Mesh
Stack Status : Active
Uptime : 1d 2h 35m
Software Version : KA.15.05
Mbr
ID  Mac Address   Model                                  Pri Status
--- ------------ ------------------------------------- --- ---------------
1   1cc1de-4d48c0 HP J9574A 3800-48G-PoE+-4SFP+ Switch   250 Commander
2   1cc1de-4d8680 HP J9573A 3800-24G-PoE+-2SFP+ Switch   230 Standby
3   1cc1de-4e3180 HP J9574A 3800-48G-PoE+-4SFP+ Switch   128 Member
4   78acc0-3c2180 HP J9576A 3800-48G-4SFP+ Switch        128 Member
```

Comware

Refer to the product information as to which models and accessory modules support IRF. Generally, IRF is supported in 10G interfaces.

All switches in an IRF configuration must be running the same version of code. Ensure this is the case before starting the IRF configuration process.

Reset the saved configurations on the Comware switches and reboot both switches.

```
<Comware>reset saved-configuration

<Comware>reboot
```

On each Comware switch, verify the IRF member is equal to 1, otherwise renumber to be member 1 and reboot the switch.

```
[Comware]display irf configuration
```

```
[Comware]member n renumber 1 (n = current member number)

<Comware>reboot
```

Configure the first switch to be the IRF master switch (Comware).

```
[Comware]irf member 1 priority 32

[Comware]interface range te1/0/49 to te1/0/52

[Comware-if-range]shutdown

[Comware-if-range]quit
```

Note - on 5900 switches, the Ten-Gig ports are in groups of four and each group of four must be defined in IRF port configurations, even if it is not planned that all four in a group will be connected.

```
[Comware]irf-port 1/1

[Comware-irf-port1/1]port group interface te1/0/49

[Comware-irf-port1/1]port group interface te1/0/50

[Comware-irf-port1/1]quit

[Comware]irf-port 1/2

[Comware-irf-port1/2]port group interface te1/0/51

[Comware-irf-port1/2]port group interface te1/0/52

[Comware-irf-port1/2]quit

[Comware]irf-port-configuration active

[Comware]save
```

Configure the second switch (Comware-2) to be the IRF slave switch.

```
[Comware-2]irf member 1 renumber 2

<Comware-2>save

<Comware-2>reboot
```

Note: When Comware-2 completes its reboot, its interfaces will now be known as G2/0/z and TenG2/0/z.

```
[Comware-2]irf member 2 priority 1

[Comware-2]interface range te2/0/49 to te2/0/52
```

```
[Comware-2-if-range]shutdown

[Comware-2-if-range]quit

[Comware-2]irf-port 2/2

[Comware-2-irf-port2/2]port group interface te2/0/49

[Comware-2-irf-port2/2]port group interface te2/0/50

[Comware-2-irf-port2/2]quit

[Comware-2]irf-port 2/1

[Comware-2-irf-port2/1]port group interface te2/0/51

[Comware-2-irf-port2/1]port group interface te2/0/52

[Comware-2-irf-port2/1]quit

[Comware-2]irf-port-configuration active

[Comware-2]interface range te2/0/49 to te2/0/52

[Comware-2-if-range]undo shutdown

[Comware-2-if-range]quit

[Comware-2]save
```

Undo shutdown on the TenG ports on the IRF master switch (Comware).

```
[Comware]interface range te1/0/49 to te1/0/52

[Comware-if-range]undo shutdown

[Comware-if-range]quit

<Comware>save
```

Note: As the IRF interfaces come up, the IRF slave switch (Comware-2) will automatically reboot.

```
[Comware]display irf ?
  >              Redirect it to a file
  >>             Redirect it to a file in append mode
  configuration  IRF configuration that will be valid after reboot
  link           Display link status
  topology       Topology information
  |              Matching output
  <cr>

[Comware] display irf
```

```
MemberID    Role    Priority  CPU-Mac         Description
 *+1        Master  32        00e0-fc0f-8c02  ---
   2        Standby 1         00e0-fc0f-8c03  ---
-------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The bridge MAC of the IRF is: cc3e-5f73-bacb
 Auto upgrade                : yes
 Mac persistent              : 6 min
 Domain ID                   : 0
 IRF mode                    : normal


[Comware] display irf configuration
MemberID NewID    IRF-Port1                      IRF-Port2
 1        1        Ten-GigabitEthernet1/0/49     Ten-GigabitEthernet1/0/51
                   Ten-GigabitEthernet1/0/50     Ten-GigabitEthernet1/0/52
 2        2        Ten-GigabitEthernet2/0/51     Ten-GigabitEthernet2/0/49
                   Ten-GigabitEthernet2/0/52     Ten-GigabitEthernet2/0/50


[Comware] display irf topology
                              Topology Info
 ---------------------------------------------------------------------
               IRF-Port1                IRF-Port2
 MemberID    Link       neighbor      Link       neighbor    Belong To
 2           DOWN       ---           UP         1           00e0-fc0f-8c02
 1           UP         2             DOWN       ---         00e0-fc0f-8c02


[Comware]display irf link
Member 1
 IRF Port  Interface                              Status
 1         Ten-GigabitEthernet1/0/49              UP
           Ten-GigabitEthernet1/0/50              UP
 2         Ten-GigabitEthernet1/0/51              DOWN
           Ten-GigabitEthernet1/0/52              DOWN
Member 2
 IRF Port  Interface                              Status
 1         Ten-GigabitEthernet2/0/51              DOWN
           Ten-GigabitEthernet2/0/52              DOWN
 2         Ten-GigabitEthernet2/0/49              UP
           Ten-GigabitEthernet2/0/50              UP
```

Cisco

Configure the first switch to be the stack master switch:

```
Cisco(config)#switch ?
  <1-9>  Switch Number

Cisco(config)#switch 1 ?
  priority   Set the priority of the specified switch
  ArubaOS-Switch  Configure Switch ArubaOS-Switch / offline config
  renumber   Renumber the specified switch number
```

```
Cisco(config)#switch 1 priority ?
  <1-15>  Switch Priority

Cisco(config)#switch 1 priority 15
Changing the Switch Priority of Switch Number 1 to 15
Do you want to continue?[confirm]
New Priority has been set successfully
```

Connect StackWise port 1 on the master switch to StackWise port 2 on the slave switch.
Connect StackWise port 2 on the master switch to StackWise port 1 on the slave switch.

Power on the slave switch.

```
Cisco#show switch detail
Switch/Stack Mac Address : 0016.c75d.8780
                                            H/W   Current
Switch#  Role   Mac Address     Priority Version  State
-----------------------------------------------------------
*1       Master 0016.c75d.8780     15     0       Ready
 2       Member 0011.2154.4b80     1      0       Ready



         Stack Port Status             Neighbors
Switch#  Port 1     Port 2           Port 1   Port 2
-----------------------------------------------------
  1        Ok         Ok                2       2
  2        Ok         Ok                1       1


Cisco#show interfaces summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface               IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
-----------------------------------------------------------------------
* Vlan1                    0     0    0     0     0    0     0    0    0
  FastEthernet1/0/1        0     0    0     0     0    0     0    0    0
  FastEthernet1/0/2        0     0    0     0     0    0     0    0    0
  FastEthernet1/0/3        0     0    0     0     0    0     0    0    0
  FastEthernet1/0/4        0     0    0     0     0    0     0    0    0
<snip>
  FastEthernet2/0/1        0     0    0     0     0    0     0    0    0
  FastEthernet2/0/2        0     0    0     0     0    0     0    0    0
  FastEthernet2/0/3        0     0    0     0     0    0     0    0    0
```

```
  FastEthernet2/0/4          0      0      0      0      0      0      0      0      0
```

Appendix A Comware Platforms – Default configuration

Before the HP 5500EI family, there were another 2 product families, i.e 3Com 4800G and H3C S5500EI, shipped to market. All three of these product families have the same hardware and software specifications except brand name and all can run the same Comware operating system.

This chapter compares the default configuration state for features or options between the two previously manufactured switch and router products from 3Com and H3C as well as the settings after the 'brand hp' command has been invoked.

Feature/Option	3Com Switch	3Com Switch 'brand hp'	3Com Router	H3C Switch	H3C Switch 'brand hp'	H3C Router
console baud rate	19200	9600	9600	9600	9600	9600
default configuration filename	3comoscfg.cfg	startup.cfg	startup.cfg	startup.cfg	startup.cfg	startup.cfg
default console login	admin no password	none	none	none	none	none
default hostname	4800G	HP	H3C	H3C	HP	H3C
default interface state	enabled	enabled	enabled	enabled	enabled	enabled
default lldp state	enabled	enabled	disabled	enabled	enabled	disabled
default PoE	enabled	disabled	n/a	disabled	disabled	n/a
default SNMP state	enabled	disabled	disabled	disabled	disabled	disabled
default SNMP version	v3	v3	v3	v3	v3	v3
default STP state	enabled	disabled	disabled	disabled	disabled	disabled
default STP version	MSTP	MSTP	MSTP	MSTP	MSTP	MSTP
telnet	enabled	disabled	disabled	enabled	disabled	disabled

3Com branded switches had the most differences in default settings when running older versions of code.

Some HP, H3C, and 3Com switches can form an HP IRF fabric (see chapter 34 and product manuals) and their MPUs are interchangeable. If different brand MPUs are used on your switch or IRF fabric, change the MPU names to be the same to prevent an active/standby MPU switchover or master re-election from causing network management problems.

Invoke the command 'brand hp' in order to configure the same HP switch id configuration to all switches in an HP IRF Fabric.

NOTE: The default settings vary with different brands. Changing the brand name might affect the running configuration. After you change the brand name of a member switch, verify the configuration and re-configure the switch if necessary.

Appendix B Comware CLI Commands in ArubaOS-Switch Software

This appendix compares Comware operations and Comware display commands added to ArubaOS-Switch software.

Included are related ArubaOS-Switch software commands and references to the corresponding Comware display command output. Refer to the latest release notes for your switch product to determine whether Comware commands are supported.

HPE Networking has added Comware CLI commands into the ArubaOS-Switch software in a phased manner over several releases to help Comware-experienced network management staff learn to use the ArubaOS-Switch software CLI with a minimum of effort.

Refer to the latest HP Switch Software – Comware CLI Commands in the ArubaOS-Switch Software reference guide.

ArubaOS-Switch K.15.13.0003 was used for this section.

a) Fundamental Commands

ArubaOS-Switch commands	Comware commands in ArubaOS-Switch Software
copy startup-config tftp <ip-address> <file name>	backup startup-configuration to <ip-address> <file name>
clock set <HH:MM:SS> <MM/DD/YYYY>	clock datetime <HH:MM:SS> <MM/DD/YYYY>
clock summer-time	clock summer-time
clock timezone	clock timezone
aaa accounting commands	command accounting
aaa authorization commands radius	command authorization
No equivalent ArubaOS-Switch software command	command-alias enable
No equivalent ArubaOS-Switch software command	command-alias mapping
copy	copy
erase startup-config	delete <startup-config>
flow-control	flow-control
console inactivity-timer	idle-timeout
exit	quit
boot	reboot
erase startup	reset saved-configuration
copy tftp startup-config	restore startup-configuration
end	return
write memory	save
reload at	schedule reboot at
reload after	schedule reboot delay
terminal length	screen-length
set authentication password	set authentication password
console baud-rate	speed
startup-default config <config file name>	startup saved-configuration <config file name>
hostname	sysname
configure	system-view
telnet	telnet
telnet-server	telnet server enable
console terminal	terminal type
no	undo

Sys-debug ip fib blackhole	No equivalent Comware software command
Sys-debug ipv6 fib blackhole	No equivalent Comware software command
Sys-debug destination logging	No equivalent Comware software command
Sys-debug destination buffer	No equivalent Comware software command
Ipv6 route <network/subnetmask> blackhole logging	No equivalent Comware software command
Ip route <network/subnetmask> blackhole logging	No equivalent Comware software command
Access-list logtimer <5-300>	No equivalent Comware software command
Sys-debug acl	No equivalent Comware software command
Sys-debug destination buffer	No equivalent Comware software command
Sys-debug destination logging	No equivalent Comware software command
vsf sequence-reboot {primary | secondary}	No equivalent Comware software command
vsf domain 20	No equivalent Comware software command
vsf lldp-mad ipv4 10.1.1.1 v2c public	No equivalent Comware software command
vsf member 4 link 1 name NAME-STR	No equivalent Comware software command
vsf member 4 link 1 all start-disabled	No equivalent Comware software command
vsf member 4 link 1 all	No equivalent Comware software command
vsf member 4 link 1	No equivalent Comware software command
vsf member 4 priority 255	No equivalent Comware software command
vsf member 4 remove reboot	No equivalent Comware software command
vsf member 4 remove	No equivalent Comware software command
vsf member 4 shutdown	No equivalent Comware software command
vsf member 4 type <jnum> mac-address <mac-ad>	No equivalent Comware software command
vsf member 4 type <jnum>	No equivalent Comware software command
vsf port-speed 1g	No equivalent Comware software command
vsf port-speed 10g	No equivalent Comware software command
vsf vlan-mad 707	No equivalent Comware software command

b) Display Commands

ArubaOS-Switch commands	Comware commands in ArubaOS-Switch Software
show arp	display arp
show arp-protection	display arp detection
show arp-protection statistics	display arp detection statistics
show arp	display arp ip-address
show flash	display boot-loader
show time show system information	display clock
show alias	display command-alias
show interface <port>	display counters
show interface <interface>	display counters rate
show cpu	display cpu-usage
No equivalent ArubaOS-Switch software command	display cpu-usage history
show running-configuration	display current-configuration
show running-configuration	display current-configuration by-linenum
No equivalent ArubaOS-Switch software command	display current-configuration configuration
show running-configuration	display current-configuration interface
show debug	display debugging
No equivalent ArubaOS-Switch software command	display default-configuration
No equivalent ArubaOS-Switch software command	display device
No equivalent ArubaOS-Switch software command	display dhcp relay information all
No equivalent ArubaOS-Switch software command	display dhcp relay information interface Vlan-interface <vlan-id>
show dhcp-relay	display dhcp relay statistics
show dhcp-snooping	display dhcp-snooping binding database
show dhcp-snooping	display dhcp-snooping information
show dhcp-snooping binding	display dhcp-snooping [ip ip_address]
show dhcp-snooping statistics	display dhcp-snooping packet statistics
show dhcp-snooping	display dhcp-snooping trust
show tech	display diagnostic-information
show ip dns	display dns domain
No equivalent ArubaOS-Switch software command	display dns domain dynamic
show ip dns	display dns < domain | server >
show port-access authenticator config	display dot1x [interface]
show port-access authenticator config	display dot1x [interface interface-list]
show port-access authenticator session counters	display dot1x sessions [interface interface-list]
show port-access authenticator statistics	display dot1x statistics [interface interface-list]
show system temperature	display environment
show system fans	display fan
show secure-mode	display fips status
show gvrp	display garp statistics interface <port_list>
show gvrp	display garp timer interface <port_list>
show gvrp	display gvrp state interface <port_list> vlan <vlan-id>
show gvrp	display gvrp statistics
show gvrp	display gvrp status
No equivalent ArubaOS-Switch software command	display gvrp vlan-operation interface interface-type interfacenumber
show history	display history-command
show tacacs	display hwtacacs

show ip igmp groups	display igmp group
show ip igmp vlan <vid>	display igmp group interface vlan-interface <vlan-id>
No equivalent ArubaOS-Switch software command	display igmp group interface vlan-interface <vlan-id> static
No equivalent ArubaOS-Switch software command	display igmp group interface vlan-interface <vlan-id> verbose
show ip igmp vlan <vid>	display igmp group port-info vlan <vlan-id>
show ip igmp vlan <vid>	display igmp group static
No equivalent ArubaOS-Switch software command	display igmp group verbose
show ip igmp vlan <vid>	display igmp group x.x.x.x static
No equivalent ArubaOS-Switch software command	display igmp group x.x.x.x verbose
show ip igmp vlan <vid>	display igmp interface
No equivalent ArubaOS-Switch software command	display igmp interface verbose
show ip igmp vlan <vid>	display igmp interface vlan-interface <vlan-id>
show ip igmp vlan <vid>	display igmp routing-table
show interface	display interface
show interfaces brief	display interface brief
show interfaces brief	display interface brief down
show ip aspath-list	display ip as-path
show dhcp-snooping bindings	display ip check source
show ip community-list	display ip community-list
No equivalent ArubaOS-Switch software command	display ip http
No equivalent ArubaOS-Switch software command	display ip https
show ip prefix-list	display ip ip-prefix
show lacp local	display lacp system-id
No equivalent ArubaOS-Switch software command	display link-aggregation load-sharing mode
No equivalent ArubaOS-Switch software command	display link-aggregation member-port
No equivalent ArubaOS-Switch software command	display link-aggregation summary
No equivalent ArubaOS-Switch software command	display link-aggregation verbose
No equivalent ArubaOS-Switch software command	display lldp local-information
No equivalent ArubaOS-Switch software command	display lldp local-information global
No equivalent ArubaOS-Switch software command	display lldp local-information interface interface-type interfacenumber
show lldp info remote-device	display lldp neighbor-information brief
show lldp info remote	display lldp neighbor-information list
show lldp info remote	display lldp neighbor-information list system-name <string>
show lldp stats	display lldp statistics
show lldp stats	display lldp statistics global
show lldp stats	display lldp statistics interface interface-type interface-number
No equivalent ArubaOS-Switch software command	display lldp status
No equivalent ArubaOS-Switch software command	display lldp status interface interface-type interface number
No equivalent ArubaOS-Switch software command	display lldp tlv-config interface interface-type interface-number
show logging	display logfile buffer
No equivalent ArubaOS-Switch software command	display loopback-detection
show mac-address	display mac-address
show system information	display mac-address aging-time
No equivalent ArubaOS-Switch software command	display mac-address multicast
show port-access mac-based	display mac-authentication
show port-access mac-based	display mac-authentication [interface …]

show system information	display memory
show uplink-failure-detection	display monitor-link group [group-number | all]
show vsf vlan-mad	No equivalent Comware software command
Show vsf	No equivalent Comware software command
Show vsf detail	No equivalent Comware software command
Show vsf link detail	No equivalent Comware software command
Show vsf link utilization	No equivalent Comware software command
Show vsf lldp-mad parameters	No equivalent Comware software command
Show vsf lldp-mad status	No equivalent Comware software command
Show vsf member <member id> link detail	No equivalent Comware software command
Show vsf member <member id> link <link id> detail	No equivalent Comware software command
Show vsf member <member id> link <link id> load-balance mac <source mac> <dest mac> inbound-port <port num>	No equivalent Comware software command
Show vsf topology change-history	No equivalent Comware software command
Show vsf topology detail	No equivalent Comware software command
Show vsf trunk-designated-forwarder member <member id>	No equivalent Comware software command
Show vsf trunk-designated-forwarder	No equivalent Comware software command
Show vsf vlan-mad	No equivalent Comware software command
No equivalent ArubaOS-Switch software command	display multicast forwarding-table
show ip mroute	display multicast routing-table
show ip pim rpf-override	display multicast routing-table static
No equivalent ArubaOS-Switch software command	display multicast rpf-info
show ip ospf statistics	display ospf cumulative
show ip ospf interface	display ospf interface
show ip ospf link-state	display ospf lsdb
show ip ospf neighbor	display ospf peer
show ip ospf	display ospf routing
show ip ospf virtual-link	display ospf vlink
show ip pim bsr	display pim bsr-info
No equivalent ArubaOS-Switch software command	display pim control-message counters
No equivalent ArubaOS-Switch software command	display pim grafts
show ip pim interface	display pim interface
show ip pim interface <interface>	display pim interface verbose
No equivalent ArubaOS-Switch software command	display pim join-prune
show ip pim neighbor	display pim neighbor
show ip pim neighbor	display pim neighbor <ip> verbose

No equivalent ArubaOS-Switch software command	display pim routing-table
No equivalent ArubaOS-Switch software command	display pim rp-info
show power-over-ethernet brief	display poe device
show power-over-ethernet brief	display poe interface
show power-over-ethernet brief	display poe interface power
show power-over-ethernet brief	display poe power-usage
show system power-supply	display poe-power alarm
No equivalent ArubaOS-Switch software command	display poe-power switch state
No equivalent ArubaOS-Switch software command	display port trunk
show system power-supply	display power
show system power-supply	display protocol-vlan
show system power-supply	display protocol-vlan interface
show crypto host-public-key show ip host-public-key	display public-key local rsa public
show ip client-public-key	display public-key peer
show radius show radius host show accoutning	display radius scheme
No equivalent ArubaOS-Switch software command	display rip
No equivalent ArubaOS-Switch software command	display rip interface
No equivalent ArubaOS-Switch software command	display rip process-id ip-address mask/mask-length
No equivalent ArubaOS-Switch software command	display rip process-id route
No equivalent ArubaOS-Switch software command	display rip process-id route peer ip-address
show rmon statistics	display rmon statistics
show route-map	display route-policy
show config	display saved-configuration
show config	display saved-configuration by-linenum
show reload <after|at>	display schedule reboot
show sflow agent	display sflow
sh sflow <receiver table number> sampling-polling	display sflow slot <slot-number>
show snmpv3 community	display snmp-agent community
show snmpv3 group	display snmp-agent group
show snmpv3 engineid	display snmp-agent local-engineid
show snmpv3 group	display snmp-agent mib-view
No equivalent ArubaOS-Switch software command	display snmp-agent statistics
show system information	display snmp-agent sys-info
show snmp-server traps	display snmp-agent trap-list
show snmpv3 user	display snmp-agent usm-user
No equivalent ArubaOS-Switch software command	display ssh client source
show ip ssh	display ssh server session
No equivalent ArubaOS-Switch software command	display ssh server-info
show ip ssh	display ssh server status
show ip ssh	display ssl client-policy
show ip ssh	display ssl server-policy
No equivalent ArubaOS-Switch software command	display startup
show spanning-tree	display stp
show spanning-tree detail show spanning-tree <port> detail	display stp abnormal-port
show spanning-tree detail	display stp bpdu-statistics
show spanning-tree detail	display stp bpdu-statistics interface GigabitEthernet <port-num>
show spanning-tree detail	display stp bpdu-statistics interface GigabitEthernet <port-num> instance <instanceNUM, 1-32>
show spanning-tree config show spanning-tree <port-list> detail	display stp brief

show spanning-tree config show spanning-tree <port-list> detail	display stp instance <instance-id> brief
show spanning-tree config show spanning-tree <port-list> detail	display stp instance <instance-id> interface GigabitEthernet <interface-id> brief
show spanning-tree config show spanning-tree <port-list> detail	display stp instance <instance-id> interface GigabitEthernet <interface-id> to GigabitEthernet <interface-id> brief
show spanning-tree config show spanning-tree <port-list> detail	display stp instance <instance-id> slot <slot-id> brief
show spanning-tree config show spanning-tree <port-list> detail	display stp interface GigabitEnterface <port-num> brief
show spanning-tree config show spanning-tree <port-list> detail	display stp interface GigabitEnterface <port-num> to GigabitEnterface <port-num> brief
No equivalent ArubaOS-Switch software command	display stp down-port
No equivalent ArubaOS-Switch software command	display stp history
No equivalent ArubaOS-Switch software command	display stp history slot <slot-number>
No equivalent ArubaOS-Switch software command	display stp instance <instance-id> history slot <slot-no>
No equivalent ArubaOS-Switch software command	display stp instance <instance-id> history
show spanning-tree	display stp
show spanning-tree	display stp instance <instance-id> interface GigabitEthernet 1/0/1
show spanning-tree	display stp slot <slot-num>
No equivalent ArubaOS-Switch software command	display stp instance <instanceid> tc
No equivalent ArubaOS-Switch software command	display stp instance <instanceid> tc slot <slot-no>
No equivalent ArubaOS-Switch software command	display stp tc
show spanning-tree mst-config	display stp region-configuration
show spanning-tree instance <instance-id> show spanning-tree detail	display stp root
show redundancy	display switchover state
show boot-history	display system-failure
No equivalent ArubaOS-Switch software command	display this
show interface transceiver detail	display transceiver alarm interface
show interface transceiver [<port>|detail]	display transceiver diagnosis interface
show interface transceiver [<port>|detail]	display transceiver interface
show interface transceiver [<port>|detail]	display transceiver manuinfo interface
show ip source-lockdown bindings	display user-bind
show vlan	display vlan
show vrrp	display vrrp
show vrrp <interface-type> vrid <virtual routerid>	display vrrp interface <interface-type> vrid <virtual routerid>
show vrrp statistics	display vrrp statistics
show vrrp statistics global	display vrrp statistics interface <interface-type> vrid <virtual routerid>
show vrrp	display vrrp verbose

Index

A

aaa accounting, 223, 245
aaa authentication, 197, 228
aaa authentication dot1x default group radius, 576
aaa authentication login privilege-mode, 217, 242
aaa authentication port-access eap-radius, 576
aaa authorization auth-proxy default group radius, 605
aaa authorization commands local, 64
aaa authorization commands radius, 221
aaa authorization console, 217, 242
aaa authorization exec default group radius, 217
aaa authorization exec default group tacacs+, 242
aaa authorization group, 64
aaa authorization network default group radius, 576
aaa common-criteria policy, 75
aaa new-model, 576, 605
aaa port-access, 576
aaa port-access mac-based, 596
aaa port-access web-based, 605
access-list, 496
accounting, 508
accounting default hwtacacs-scheme, 228
accounting default radius-scheme, 198
accounting lan-access radius-scheme radius-auth, 576
accounting portal radius-scheme radius-auth, 605
acl number, 479, 489, 503
acl number 2000, 479, 489, 503
acl number 3000, 479, 489, 503
acl number 4000, 495
action drop, 495, 496
action forward, 496
active region-configuration, 398, 400
area, 442
area 1, 444
area 1 stub, 444
area 2 stub, 445
area 2 stub no-summary, 445
arp detection enable, 562
arp detection trust, 562
arp rate-limit, 569
arp source-suppression, 569
arp source-suppression enable, 569
arp-protect, 562
authentication default hwtacacs-scheme, 228
authentication default radius-scheme, 198
authentication lan-access radius-scheme radius-auth, 576
authentication portal radius-scheme radius-auth, 605
authorization default hwtacacs-scheme, 228
authorization default radius-scheme, 198
authorization lan-access radius-scheme radius-auth, 576
authorization portal radius-scheme radius-auth, 605

B

backup startup-configuration, 100
banner motd, 40
bgp 64502, 454
bgp router-id 10.0.0.21, 454
boot config-file, 102
boot set-default flash primary, 86
boot system flash, 86
boot-loader file flash, 86
Bridge-Aggregation, 375
bsr-candidate source-ip-vlan, 530

C

c-bsr Vlan-interface, 530
channel-group, 382
class all_traffic, 519
class-map all_traffic, 519
clear line, 33
clock, 124, 134
clock protocol ntp, 125
configure, 14
configure terminal, 14
connection-rate-filter sensitivity, 569
console baud-rate, 15
console inactivity-timer, 8, 16
copy config, 101
copy flash, 86, 101
copy flash sftp, 86
copy flash tftp, 86
copy running-config, 100
copy running-config sftp, 100
copy running-config tftp, 100
copy sftp, 85
copy startup-config, 100
copy startup-config sftp, 100
copy startup-config tftp, 100

copy tftp, 85
copy tftp startup-config, 101
c-rp Vlan-interface, 530
crypto key generate, 172

D

deny ip, 479, 489, 496, 503, 606
description link_to_core, 288
dhcp enable, 329
dhcp relay, 329
dhcp relay server-address 10.0.100.251, 329
dhcp select relay, 329
dhcp snooping enable, 552
dhcp-snooping, 552
dir, 23, 85, 102
dir usba0:/, 23
disable, 288
display arp detection, 562
display arp source-suppression, 569
display bgp peer, 454
display boot-loader, 102
display clock, 124, 125
display current-configuration, 38, 100
display device manuinfo, 25
display device usb, 23
display dhcp relay, 329
display dhcp relay server-address, 329
display dhcp-snooping, 552
display diagnostic-information, 8, 36
display dldp, 544
display dot1x, 577
display environment, 25
display fan, 25, 33
display hwtacacs, 229
display interface, 288, 310, 368
display ip interface brief, 327
display irf, 636
display irf configuration, 635, 637
display irf link, 637
display irf topology, 637
display job, 280
display link-aggregation, 375, 382
display lldp neighbor-information, 249, 256
display lldp neighbor-information interface M-GigabitEthernet 0/0/0, 266
display lldp neighbor-information list, 249
display logbuffer, 117
display mac-authentication, 597
display mirroring-group, 619, 626
display mvrp running-status, 351
display mvrp state interface, 351
display ntp-service sessions, 124
display ntp-service status, 125
display ospf, 446
display password-control, 75
display pim, 526, 530
display poe device, 362
display poe interface, 362
display portal connection statistics al, 607
display power, 25
display private-vlan, 336
display qos, 508
display radius scheme, 198
display radius statistics, 198
display rip, 434
display role name, 64
display schedule reboot, 18
display scheduler, 18
display scheduler job, 280
display scheduler schedule, 280
display snmp-agent, 153
display snmp-agent sys-info, 140
display ssh server, 173
display startup, 60, 102
display stp, 387, 399, 400, 422
display stp root, 422
display users, 30, 166
display version, 85
display vlan, 304, 310, 368, 375, 382, 577
display voice vlan, 369
display vrrp, 471
display web users, 183
dldp enable, 544
dldp global enable, 544
domain 8021x, 576
domain default enable lab, 198
domain tacacs, 229
domain web-auth, 605
dot1x, 576
dot1x mac-auth-bypass, 596
dot1x system-auth-control, 576
duplex auto, 288

E

enable, 13, 288, 471
enable password, 44
enable secret, 44
encapsulation s-vid 2, 359
erase startup-config, 101
exec-timeout, 16

F

feature nv overlay, 359
file prompt quiet, 280
filter connection-rate, 569
free user-interface vty, 33

H

header motd, 40
hwtacacs scheme tacacs_auth, 227, 229

I

idle-timeout, 16
if-match any, 508
igmp enable, 540
import-route direct, 434
import-route static, 466
info-center loghost, 117
info-center loghost source Vlan-interface, 41
info-center timestamp loghost date, 117
instance, 398
interface, 288, 310, 362, 368, 375, 382, 503, 508, 519, 544
interface 11 monitor all both mirror 1, 619
interface Bridge-Aggregation, 374, 382
interface fastEthernet 0, 264
interface M-GigabitEthernet 0/0/0, 265
interface port-channel, 374, 382
interface tunnel, 359
interface vlan, 327, 329, 445, 471, 489, 490, 526, 530
interface Vlan-interface, 327, 329, 445, 526, 530
ip <service> source-interface, 41
ip access-group, 489, 490, 495, 496, 503
ip access-group 101, 504
ip access-group 11, 503
ip access-group ext_acl, 504
ip access-group std_acl, 503
ip access-group std_acl in, 489
ip access-group web-auth-policy1 in, 606
ip access-list, 519
ip access-list extended, 479, 489, 496, 503
ip access-list extended ext_acl, 479, 490, 496, 503
ip access-list extended web-auth-policy1, 606
ip access-list standard, 479, 489, 495, 503
ip access-list standard std_acl, 479, 489, 503
ip address, 327
ip admission name web-auth-rule1 proxy http, 605
ip admission web-auth-rule1, 606
ip arp inspection, 562
ip arp inspection limit, 569
ip dhcp snooping, 552, 562
ip helper-address, 329
ip http enable, 183
ip http secure-server, 188
ip http server, 183
ip https enable, 188
ip igmp, 540
ip multicast-routing, 526, 530
ip multicast-routing distributed, 526, 530
ip ospf area, 442
ip ospf cost, 445
ip pim bsr-candidate vlan, 530
ip pim dense-mode, 526
ip pim rp-candidate vlan, 530
ip pim sparse-mode, 530
ip pim-dense, 526
ip pim-sparse, 530
ip router-id, 439
ip source-interface, 41
ip ssh, 172
ip ssh listen oobm, 265
ip ssh source-interface fastEthernet 0, 265
ip telnet source-interface fastEthernet 0, 265
ip tftp source-interface fastEthernet 0, 265
irf member 1 priority 32, 635
irf-port, 635
irf-port-configuration active, 635

J

job, 280

K

key accounting password, 197
key authentication password, 575, 596
kill, 33
kron occurrence, 280

kron policy-list, 280

L

l2vpn enable, 359
line console, 15
line vty, 172
link-aggregation mode dynamic, 374
link-keepalive, 544
lldp compliance cdp, 256
lldp enable, 249
lldp global enable, 250
lldp run, 9, 249
local-user, 44
logging, 117
logging console, 117
logging facility, 117
logging severity, 117
loopback-detection enable, 549
loopback-detection global enable, 549
loop-protect, 549
lower-case, 75

M

mac-authentication, 596
match access-group, 519
match ip address, 495, 496
max-length, 75
member n renumber 1, 635
member vni, 359
min-length, 75
mirror 1 port 12, 619
mirroring-group, 625
mirroring-group 1 local, 619
mirroring-group 1 mirroring-port g1/0/18 both, 619
mls qos, 508
mls qos cos, 508
mls qos map dscp-cos, 508
mls qos trust dscp, 508
mode vxlan, 359
monitor session 1 destination interface f1/0/12
encapsulation replicate, 619
monitor session 1 source interface f1/0/6 both, 619
multicast routing-enable, 526, 530
mvrp enable, 351
mvrp global enable, 351

N

name link_to_core, 288
name ArubaOS-Switch-Comware-Cisco, 398
name test, 304
name voice, 368
neighbor 10.0.111.31 remote-as 64502, 454
neighbor 10.0.112.1 next-hop-self, 466
network, 434, 439, 442
no front-panel-security password, 60
no ip http server, 188
no reload, 18
no service password-recovery, 60
no shutdown, 288, 327
no web-management plaintext, 188
ntp enable, 124
ntp server, 124
ntp source fastEthernet 0, 265
ntp source M-GigabitEthernet 0/0/0, 265
ntp unicast, 124
ntp-service, 124
ntp-service enable, 124
ntp-service unicast-server, 124
numeric-count, 75

O

oobm, 264
ospf 1 router-id, 439
ospf cost, 445

P

parser view, 64
password complexity all, 75
password configuration aging, 75
password configuration history, 75
password configuration-control, 75
password manager user-name, 44
password minimum-length, 75
password-control complexity same-character check, 75
password-control complexity user-name check, 75
password-control composition, 75
password-control composition enable, 75
password-control enable, 75
password-control length, 75
peer 10.0.111.21 as-number 64501, 454
peer 10.0.113.1 next-hop-local, 466

permit, 479, 489, 495, 503
permit icmp, 496
permit ip, 479, 490, 496, 503, 519
permit tcp, 606
permit udp, 606
pim, 530
pim dm, 526
pim sm, 530
poe enable, 362
policy-list, 280
policy-map rate_limit, 519
port, 310
port group interface, 635
port hybrid, 368
port link-aggregation, 375
port link-aggregation group, 382
port link-type, 368
port link-type trunk, 310, 375, 626
port private-vlan, 336
port private-vlan host, 336
port trunk, 626
port trunk permit, 310, 382
port trunk permit vlan, 375
power inline auto, 362
power inline never, 362
primary accounting, 228, 575, 596
primary authentication, 228, 575, 596
primary authorization, 228
private-vlan association add, 336
private-vlan community, 336
private-vlan isolated, 335
private-vlan primary, 335
private-vlan promiscuous, 336
private-vlan secondary, 336
public-key local create rsa, 172

Q

qos lr outbound cir, 519
qos policy, 508
qos priority, 508
qos trust dscp, 508
qos type-of-service diff-services, 508
qos vlan-policy, 508

R

radius scheme, 575, 596
radius scheme, 197, 199
radius-server, 575, 596, 605
radius-server host, 197, 575, 596, 605
rate-limit all in percent, 519
rate-limit all out, 519
reboot, 18
redistribute, 439
redistribute connected, 434
region-name ArubaOS-Switch-Comware-Cisco, 398
reload, 18
remote-span, 625
reset saved-configuration main, 101
revision, 398
revision-level, 398
rip, 434
role name, 64
router bgp 64501, 454
router ospf, 439, 442
router pim, 526, 530
router rip, 434
router-id, 439
router-id 10.0.0.31, 454
rp-address, 530
rp-candidate source-ip-vlan, 530
rule deny ip, 479, 489, 503
rule permit source, 479, 489, 503

S

schedule reboot, 18
scheduler job, 280
scheduler reboot, 18
scheduler schedule, 280
server-type extended, 575, 596, 605
service-instance, 359
show aaa common-criteria policy name, 75
show aaa servers, 198
show aaa user all, 223, 246
show accounting, 223
show arp-protect, 562
show authentication, 229, 242
show authorization group, 64
show boot, 102
show cdp, 256
show clock, 124
show config files, 102
show connection-rate-filter, 569
show crypto host-cert, 188

show crypto host-public-key, 173
show crypto key mypubkey rsa, 173
show crypto pki certificates verbose, 188
show dhcp-relay, 329
show dhcp-snooping, 552
show dot1x, 577
show dot1x interface, 597
show env fan, 25, 33
show env power, 25
show env temperature, 25
show etherchannel, 382
show flash, 85, 102
show front-panel-security, 60
show interface private-vlan mapping, 337
show interfaces, 288, 310, 368, 375
show inventory, 25
show ip, 327, 526, 530
show ip admission cache, 607
show ip arp, 562
show ip arp inspection interfaces, 569
show ip bgp summary, 454
show ip dhcp snooping, 552
show ip helper-address, 329
show ip host-public-key, 173
show ip interface, 329
show ip interface brief, 327
show ip ospf, 446
show ip rip, 434
show ip ssh, 173
show job, 280
show job save-config, 280
show kron schedule, 280
show lacp, 375
show lldp info remote-device, 249
show lldp info remote-device oobm, 265
show lldp neighbors, 249
show lldp neighbors fastEthernet 0, 265
show logging, 117
show mls qos, 508
show modules, 25
show monitor, 619, 625, 626
show mvrp config, 351
show mvrp state, 351
show ntp associations, 124
show ntp status, 124
show password-configuration, 75
show port-access authenticator, 577
show port-access mac-based, 597
show port-access web-based config, 607
show power inline, 362
show power-over-ethernet, 362
show qos, 508
show radius, 198
show radius authentication, 198
show radius host, 198
show radius statistics, 198
show run, 38
show running-config, 100
show snmp, 140, 153
show snmp-server, 140
show snmpv3, 153
show sntp, 134
show spanning-tree, 387, 399, 422
show spanning-tree root, 422
show spanning-tree summary, 422
show stacking, 634
show switch detail, 638
show system fans, 25, 33
show system power-supply, 25
show system temperature, 25
show tacacs, 229
show tech, 8, 36
show tech-support, 8, 36
show telnet, 30, 166
show time, 124
show trunks, 382
show usb-port, 23
show users, 30, 166
show version, 60, 85
show vlan, 310
show vlan brief, 304, 577
show vlan private-vlan, 337
show vlan private-vlan type, 337
show vlans, 304, 310, 368, 382, 577
show vlans private-vlan, 336
show vrrp, 471
shutdown, 288
snmp-agent, 140
snmp-agent group v3, 153
snmp-agent trap source Vlan-interface, 41
snmp-server, 140
snmp-server group <name> v3, 153
snmp-server trap-source, 41
snmpv3, 153

sntp, 134
sntp enable, 134
sntp server priority, 134
sntp unicast-server, 134
spanning-tree, 387, 398, 399, 421
spanning-tree 6 bpdu-filter, 548
spanning-tree 6 root-guard, 551
spanning-tree 6 tcn-guard, 551
spanning-tree bpdufilter enable, 548
spanning-tree bpduguard enable, 548
spanning-tree bpdu-protection-timeout, 548
spanning-tree guard loop, 549
spanning-tree guard root, 551
spanning-tree instance, 399
spanning-tree mode, 398
spanning-tree mode rapid-pvst, 421
spanning-tree vlan 1 priority 1, 421
special-case, 75
speed, 15
speed auto, 288
speed-duplex auto, 288
srr-queue bandwidth limit, 519
ssh client source interface M-GigabitEthernet 0/0/0, 265
ssh server enable, 172
stacking member 1 priority 255, 634
stacking set-stack, 634
startup saved-configuration, 102
startup-default primary, 102
stp bpdu-protection, 548
stp cost, 387
stp edged-port enable, 387
stp enable, 387, 398, 421
stp global enable, 422
stp instance, 399
stp mode pvst, 421, 422
stp mode rstp, 387, 388
stp port priority, 387
stp priority, 387, 399
stp region-configuration, 398, 399
stp root-protection, 551
stp vlan 220 priority 4096, 421
stub no-summary, 445
super password level 3, 44
super password role network-admin, 45
switch 1 priority 15, 638
switchport, 310, 368
switchport mode access, 375, 382, 576, 606
switchport mode private-vlan host, 336
switchport mode private-vlan promiscuous, 336
switchport nonegotiate, 310, 375, 382
switchport trunk, 310, 374, 382
switchport trunk encapsulation dot1q, 625
system-view, 13

T

tacacs-server host, 228
tagged, 310
telnet client source interface M-GigabitEthernet 0/0/0, 265
telnet server enable, 165
telnet-server listen oobm, 264
timesync ntp, 124
traffic behavior, 508
traffic classifier, 508
trunk, 374, 382
tunnel destination, 359
tunnel mode vxlan, 359
tunnel source, 359

U

udld port, 544
undo dot1x handshake, 576
undo poe enable, 362
undo schedule reboot, 18
undo scheduler reboot, 18
undo shutdown, 288
undo startup bootrom-access enable, 60
untagged, 310
upper-case, 75
user-interface aux 0, 15
user-interface vty, 172, 221
username, 44, 183
user-name-format without-domain, 575, 596

V

version 2, 434
virtual-ip-address, 471
virtual-network, 359
vlan, 304, 327, 329, 368, 445, 471, 489, 490, 495, 496, 508, 526
vlan access-map, 495, 496
vlan filter, 495, 496
vn-segment, 359
voice, 368

vrrp vrid, 471
vsi, 359
vtp mode transparent, 335
vxlan enable, 359
vxlan tunnel, 359
vxlan udp, 359

W

web-management listen oobm, 265
web-management plaintext, 183
web-management ssl, 188

X

xconnect vsi, 359

a Hewlett Packard Enterprise company

♥ Copyright 2017 Aruba, a Hewlett Packard Enterprise Company

The information contained herein is subject to change without notice. The only warranties for Aruba products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Aruba shall not be liable for technical or editorial errors or omissions contained herein.

This is an Aruba cop3righted work that may not be reproduced without the written permission of Aruba. You may not use these materials to deliver training to any person outside of your organization without the written permission of Aruba.

Printed in the United States of America

ArubaOS-Switch, Comware and Cisco IOS CLI Reference Guide
Version 3.3

For more information

http://www.arubanetworks.com/

3315 Scott Blvd| Santa Clara, CA 95054

1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | info@arubanetworks.com

www.arubanetworks.com