ArubaOS-Switch and Cisco IOS CLI Reference Guide

aruba
a Hewlett Packard Enterprise company

Table of Contents

Introduction 5
Using This Guide 6
Navigation Differences Among CLIs 6
Configuration Differences Among CLIs 6
Terminology Differences 7
Disclaimer 7
Comparing View and Configuration Prompts 8
Comparing Frequently Used Commands 8
Chapter 1 Basic Switch Management 9
a) Management Access 9
b) Configuration Access 10
c) Console Access—Baud Rate 11
d) Console and Virtual Terminal Access—Timeout 11
e) Reload & Timed Reload 12
f) USB 14
g) System and Environment 15
h) Remote Management Sessions—Viewing 19
i) Remote Management Sessions—Terminating 20
j) Tech Support Information Output Listing 21
k) Filtering Output show running-config and display current-configuration 22
l) Motd 23
m) Source Interface for Management Communications 23
Chapter 2 Switch User ID and Password, and Console Access 26
a) Local User ID and Password, and console access 26
b) Recover Lost Password 30
c) Protect Local Password 31
d) Role based management 33
e) Password complexity 40
Chapter 3 Image or Operating System File Management 46
Chapter 4 Configuration File Management 55

Chapter 5 Syslog Services 64
Chapter 6 Time Service 69
a) NTP 69
b) SNTP 73
Chapter 7 SNMP 77
a) SNMP Version 1 and Version 2c 78
b) SNMP Version 3 85
Chapter 8 CLI Management Access – Telnet and SSH 92
a) Telnet 92
b) SSH 94
Chapter 9 GUI Management Access – HTTP and HTTPS 99
a) HTTP 99
b) HTTPS - SSL (Self-Signed Certificates) 100
Chapter 10 RADIUS Authentication for Switch Management 106
a) Basic Configuration 107
b) Privilege Mode 116
c) Commands Authorization 119
d) RADIUS Accounting 120
Chapter 11 TACACS+/HWTACACS Authentication for Switch Management 123
a) Basic Configuration 123
b) Privilege Mode 129
c) TACACS Accounting 131
Chapter 12 Discovery Protocols – LLDP and CDP 135
a) LLDP 135
b) CDP 139
Chapter 13 Out-of-Band Management 143
Chapter 14 Job Schedule 154
Chapter 15 Interface or Port Information and Nomenclature 158
Chapter 16 VLAN Management 167
a) Creating and Naming VLANs 167
b) Assigning Ports or Interfaces to VLANs 170

c) Assigning an IP Address to a VLAN 177
d) IP Helper to Relay / Forward DHCP Requests 179
Chapter 17 Advanced VLAN Features 182
a) Private VLAN 182
b) MVRP 183
c) VxLAN 184
d) MDNS, IPv6 ND snooping, BFD 185
e) RIPNG 187
f) IP-SLA, Portscan detection 188
g) Federal Govt Certification, Netdestination 193
Chapter 18 PoE (Power over Ethernet) 196
Chapter 19 VoIP Support 201
Chapter 20 Link Aggregation – LACP and Trunk 203
a) Link Aggregation Control Protocol (LACP) 203
b) Trunk 208
Chapter 21 RSTP 212
Chapter 22 MSTP 217
Chapter 23 PVST/PVST+/RPVST/RPVST+ 228
Chapter 24 RIP – v1 and v2 233
Chapter 25 OSPFv2 236
a) Single Area 236
b) Multiple Areas 238
c) Stub 240
d) Totally Stubby 240
e) Show or Display OSPF Commands 241
Chapter 26 BGP version 4 246
a) eBGP 247
b) iBGP 253
Chapter 27 VRRP 256
Chapter 28 ACLs 260
a) Definitions of Standard or Basic ACLs and Extended or Advanced ACLs 260

b) ACL Fundamental Configuration Options 260
Standard/Basic 260
Extended/Advanced 261
c) Routed/Layer 3 ACL (RACL) 261
Standard or Basic ACL 262
Extended or Advanced ACL 262
d) VLAN/Layer 2 Based ACL (VACL) 265
Standard or Basic ACL 265
Extended or Advanced ACL 265
e) Port ACL (PACL) 269
Standard or Basic ACL 269
Extended or Advanced ACL 269
Chapter 29 QoS 272
QoS Operational Characteristics 272
a) QoS 273
b) Rate Limiting 277
Chapter 30 IP Multicast 281
a) PIM Dense 282
b) PIM Sparse 284
c) IGMP 289
Chapter 31 Spanning Tree Hardening 290
a) UDLD and DLDP 292
b) BPDU Protection and BPDU Guard 294
c) Loop Protection 295
d) Root Guard 295
Chapter 32 DHCP Snooping 296
Chapter 33 ARP Protection, ARP Detection, and Dynamic ARP Inspection 301
Chapter 34 Connection Rate Filtering 306
Chapter 35 802.1X Authentication 309
a) 802.1X Authentication 309

b) MAC Authentication 311
c) Web or Portal Authentication 316
Chapter 36 Port Mirroring or Port Span 325
a) Local Mirror or SPAN 325
b) Remote Mirror or RSPAN 329
Chapter 37 Tunneled Node, Trust QoS, Clear Pass Intergration 334
Chapter 38 HP 3800 Stacking / HP IRF / Cisco Switch Stacks 338
Appendix A CLI Commands in ArubaOS-Switch Software 342
a) Fundamental Commands 342
b) Display Commands 343
Index 348

ArubaOS-Switch 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 two switch operating systems: HPE ArubaOS-Switch (now the Aruba OS), and Cisco IOS operating systems.

In this guide, we refer to HPE ProVision as ArubaOS-Switch 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 commands included in this guide were tested on the following:

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

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.

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 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 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, 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. 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 Cisco it is *EtherChannel*.

Interface use	ArubaOS-Switch	Cisco
Non-802.1Q interfaces (such as used for computers or printers)	`untagged`	`access`
802.1Q interfaces (such as used for switch-to-switch, switch-to-server, and switch-to-VoIP phones)	`tagged`	`trunk`
Aggregated interfaces	`trunk`	`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	Cisco
U = User Exec / User View	ArubaOS-Switch>	Cisco>
P = Privileged Exec	ArubaOS-Switch#	Cisco#
S = System View (equal to Priviledged Exec)		
C = Configuration	ArubaOS-Switch(config)#	Cisco(config)#

Comparing Frequently Used Commands

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

	ArubaOS-Switch		Cisco
U	enable	U	enable
P	configure	U	configure terminal
U/P/C	show flash	U/P	show flash
U/P/C	show version	U/P	show version
P/C	show run	P	show run
P/C	show config	P	show start
U/P/C	show history	U/P	show history
U/P/C	show logging	U/P	show logging
U/P/C	show ip route	U/P	show ip route
U/P/C	show ip	U/P	show ip interface brief
U/P/C	show interface brief	U/P	show interfaces status
P/C	erase startup-config	P	erase start
P/C	show config <filename>	P	more flash:/<filename>
P/C	reload	P	reload
P/C	write memory	P	write memory
P	show tech	U/P	show tech-support
U/P/C	show	U/P	show
U/P/C	no	P	no
C	end	C	end
U/P/C	exit	U/P/C	exit
P/C	erase	P	erase
P/C	copy	P	copy
C	hostname	C	hostname
C	logging	C	logging
C	router rip	C	router rip
C	router ospf	C	router ospf
C	ip route	C	ip route
C	access-list	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	Cisco
`ArubaOS-Switch> enable`	`Cisco> enable`
`ArubaOS-Switch#`	`Cisco#`

ArubaOS-Switch

`ArubaOS-Switch> enable`
 	
`ArubaOS-Switch#`

Cisco

`Cisco> enable`
 	
`Cisco#`

b) Configuration Access

ArubaOS-Switch	Cisco
ArubaOS-Switch# configure	Cisco# configure terminal Enter configuration commands, one per line. End with CNTL/Z.
ArubaOS-Switch(config)#	Cisco(config)#

ArubaOS-Switch

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

ArubaOS-Switch# configure

ArubaOS-Switch(config)#
```

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	Cisco
ArubaOS-Switch(config)# console baud-rate ?	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)#
```

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	Cisco
ArubaOS-Switch(config)# console inactivity-timer ?	Cisco(config)#line console 0
	Cisco(config-line)#exec-timeout ?
	[also]
	Cisco(config)#line vty 0
	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.

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	Cisco
ArubaOS-Switch# reload	Cisco#reload
ArubaOS-Switch# reload ?	Cisco#reload ?
ArubaOS-Switch# show reload ?	Cisco#show reload
ArubaOS-Switch(config)# no reload	Cisco#reload cancel

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
```

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	Cisco
	not an available feature
ArubaOS-Switch# dir	
ArubaOS-Switch# show usb-port	

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)
```

Cisco

not an available feature

g) System and Environment

ArubaOS-Switch	Cisco
ArubaOS-Switch# show system information ArubaOS-Switch# show modules	Cisco#show inventory Cisco#show version
ArubaOS-Switch# show system fans	Cisco#show env fan
ArubaOS-Switch# show system power-supply	Cisco#show env power
ArubaOS-Switch# show system temperature	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
```

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	Cisco
ArubaOS-Switch# show telnet	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       :
```

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	Cisco
ArubaOS-Switch# kill 3	Cisco# clear line 3
	Cisco# clear line vty 2

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       :
```

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	Cisco
ArubaOS-Switch# show tech	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>
```

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	Cisco
Note: entering `show running-config | ?` does not reveal this command operation	
	`Cisco#show running-config | ?`
`ArubaOS-Switch# show running-config | 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>
```

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	Cisco
ArubaOS-Switch(config)# banner motd # Enter TEXT message. End 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!
#
```

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	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	Cisco(config)#logging source-interface vlan 1
ArubaOS-Switch(config)# ip source-interface radius 10.0.111.21	Cisco(config)#ip radius source-interface vlan 1
ArubaOS-Switch(config)# ip source-interface tacacs 10.0.111.21	Cisco(config)#ip tacacs source-interface vlan 1
	Cisco(config)#ip ftp source-interface vlan 1
ArubaOS-Switch(config)# ip source-interface tftp vlan 1	Cisco(config)#ip tftp source-interface vlan 1
ArubaOS-Switch(config)# ip source-interface sntp vlan 1	Cisco(config)#ntp source vlan 1
ArubaOS-Switch(config)# ip source-interface telnet vlan 1	Cisco(config)#ip telnet source-interface vlan 1
	Cisco(config)#ip ssh source-interface vlan 1
ArubaOS-Switch(config)# ip source-interface sflow 10.0.111.21	
ArubaOS-Switch(config)# snmp-server trap-source 10.0.111.21	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
```

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, 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	Cisco
	Cisco(config)#enable password 0 <password>
	Cisco(config)#enable secret 0 <password>
ArubaOS-Switch(config)# password manager user-name <name> plaintext <password>	Cisco(config)#username <name> privilege 15 password <password>
ArubaOS-Switch(config)# password operator user-name <name> plaintext <password>	Cisco(config)#username <name> privilege 0 password <password>
	Cisco(config)#line console 0 Cisco(config-line)#login local
	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

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.

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	Cisco
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).
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	Cisco
ArubaOS-Switch(config)# no front-panel-security password-clear	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	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.

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	Cisco
	Cisco(config)#aaa new-model
ArubaOS-Switch(config)# aaa authorization commands local	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	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	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: ********	Cisco(config-view)#exit Cisco(config)#username test1 privilege 15 view network-admin2 password 0 password
ArubaOS-Switch# show authorization group network-admin2	(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
```

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	Cisco
ArubaOS-Switch(config)# password minimum-length 10	Cisco(config)#aaa new-model
ArubaOS-Switch(config)# password configuration-control	Cisco(config)#aaa common-criteria policy pwcomplex
ArubaOS-Switch(config)# password configuration aging	Cisco(config-cc-policy)#min-length 10
ArubaOS-Switch(config)# password configuration history	Cisco(config-cc-policy)#max-length 10
ArubaOS-Switch(config)# password complexity all	Cisco(config-cc-policy)#numeric-count 2
	Cisco(config-cc-policy)#special-case 2
	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	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
```

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, 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.)

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-Switches can store a maximum of two operating system files. With 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	Cisco
ArubaOS-Switch# show flash	Cisco#show flash:
ArubaOS-Switch# show version	Cisco#show version
ArubaOS-Switch# copy tftp flash 10.0.100.111 K_15_16_0004.swi	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: ********	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	
ArubaOS-Switch# copy xmodem flash	Cisco#copy xmodem: flash:
ArubaOS-Switch# copy flash flash secondary	
ArubaOS-Switch# copy flash tftp 10.0.100.111 K_15_16_0004.swi	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: ********	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	
ArubaOS-Switch# copy flash xmodem	
ArubaOS-Switch# boot set-default flash primary	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.
```

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, 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.)

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. 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	Cisco
ArubaOS-Switch# show running-config ?	Cisco#show running-config ?
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	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 Attempting username/password authentication... Enter manager@10.0.100.111's password: ********	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:
ArubaOS-Switch# copy config config1 config config2	Cisco#copy flash:Cisco.cfg flash:Cisco_2.cfg
ArubaOS-Switch# copy config config1 tftp 10.0.100.111 config1.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	Cisco#copy flash:Cisco.cfg scp: Address or name of remote host []? 10.0.100.111

Attempting username/password authentication... Enter manager@10.0.100.111's password: ********	Destination username [manager]? Destination filename [Cisco.cfg]? Writing Cisco.cfg Password:
ArubaOS-Switch# erase startup-config	Cisco#erase startup-config
ArubaOS-Switch# copy tftp startup-config 10.0.100.111 config6.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: ********	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	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: ********	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	Cisco#show flash Cisco#show boot
ArubaOS-Switch# startup-default config config1	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
```

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	Cisco
ArubaOS-Switch(config)# logging 10.0.100.111	Cisco(config)#logging 10.0.100.111
ArubaOS-Switch(config)# logging facility ?	Cisco(config)#logging facility ?
ArubaOS-Switch(config)# logging severity ?	Cisco(config)#logging console ?
	Cisco(config)#service timestamps log datetime localtime
ArubaOS-Switch# show logging ?	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>
```

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	Cisco
ArubaOS-Switch(config)# ntp 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	Cisco#show ntp associations
ArubaOS-Switch# show ntp 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	Cisco(config)# clock summer-time US-Cent date mar 8 2015 02:00 nov 1 2015 02:00 60
ArubaOS-Switch# show time	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]

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
```

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	Cisco
ArubaOS-Switch(config)# sntp server priority 1 10.0.100.251	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	

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
```

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 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	Cisco
[snmp v1/v2c is default version]	
ArubaOS-Switch(config)# snmp-server host 10.0.111.210 community private trap-level all	Cisco(config)#snmp-server host 10.0.111.210 version 2c private
ArubaOS-Switch(config)# snmp-server community public operator restricted	Cisco(config)#snmp-server community public ro
ArubaOS-Switch(config)# snmp-server community private manager unrestricted	Cisco(config)#snmp-server community private rw
ArubaOS-Switch(config)# snmp-server location Lab	Cisco(config)#snmp-server location Lab
ArubaOS-Switch(config)# snmp-server contact Lab_Engr	Cisco(config)#snmp-server contact Lab_Engr
ArubaOS-Switch(config)# snmp-server enable	Cisco(config)#snmp-server enable traps
ArubaOS-Switch# show snmp-server	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
```

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	Cisco
ArubaOS-Switch(config)# snmpv3 enable	
	Cisco(config)#snmp-server group <name> v3 priv
ArubaOS-Switch(config)# snmpv3 user test auth md5 password priv 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	Cisco(config)#snmp-server host 10.0.111.210 version 3 priv test
ArubaOS-Switch(config)# snmp-server location Lab	Cisco(config)#snmp-server location Lab
ArubaOS-Switch(config)# snmp-server contact Lab_Engr	Cisco(config)#snmp-server contact Lab_Engr
ArubaOS-Switch# show snmpv3 enable ArubaOS-Switch# show snmpv3 targetaddress	Cisco#show snmp host
ArubaOS-Switch# show snmpv3 user	Cisco#show snmp user
ArubaOS-Switch# show snmpv3 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
```

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 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	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.	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.

	`Cisco(config)#line vty 0 15`
	
	`Cisco(config-line)#login local`

	`Cisco(config)#line vty 0 15`
	
	`Cisco(config-line)#login`
	
	`Cisco(config-line)#password 0 password`

`ArubaOS-Switch# show telnet`	`Cisco#show users`

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       :
```

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	Cisco
	Cisco(config)#hostname Cisco
	Cisco(config)#ip domain-name test
ArubaOS-Switch(config)# crypto key generate ssh	Cisco(config)#crypto key generate
ArubaOS-Switch(config)# ip ssh	Cisco(config)#ip ssh version 2
	Cisco(config)#line vty 0 15 Cisco(config-line)#login local Cisco(config-line)#transport input ssh
	Cisco(config)#username <name> privilege 15 password <password>
ArubaOS-Switch(config)# no telnet-server	(NOTE: by configuring 'transport input ssh' on the vty interfaces, telnet access is disabled)
ArubaOS-Switch# show ip ssh	Cisco#show ip ssh Cisco#show ssh
ArubaOS-Switch# show crypto host-public-key	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==
```

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).

You can find configuration details for User ID's and Password's in Chapter 2.

a) HTTP

ArubaOS-Switch	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.	HTTP server is enabled by default, but must configure http authentication type. Must have all the device web files for full functionality.
	`Cisco(config)#username <name> privilege 15 password <password>`
	`Cisco(config)#ip http authentication local`
`ArubaOS-Switch(config)# web-management plaintext`	`Cisco(config)#ip http server`
	`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.

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	Cisco
	`http secure-server` is enabled by default and a self-signed certificate is automatically generated

ArubaOS-Switch(config)# crypto pki enroll-self-signed certificate-name localcert subject	Cisco(config)#crypto key generate rsa
ArubaOS-Switch(config)# web-management ssl	Cisco(config)#ip http secure-server
ArubaOS-Switch(config)# no web-management plaintext	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
	Cisco#show ip http server connection

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
```

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	Cisco
	Cisco(config)#radius server radius-auth
ArubaOS-Switch(config)# radius-server host 10.0.100.111 key password	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	
	Cisco(config)#line vty 0 15
	Cisco(config-line)#login authentication default
ArubaOS-Switch# show radius	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	Cisco#show 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
```

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	Cisco
(Requires special configuration on the RADIUS server)	(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
```

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	Cisco
(Requires special configuration on the RADIUS server)	Not an available feature
`ArubaOS-Switch(config)# aaa authorization commands radius`	
`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
```

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	Cisco
ArubaOS-Switch(config)# aaa accounting exec start-stop radius	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'
```

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	Cisco
	`Cisco(config)#aaa new-model`
`ArubaOS-Switch(config)# tacacs-server host 10.0.100.111 key password`	`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+
	Cisco(config)#line vty 0 15
	Cisco(config-line)#login authentication default
ArubaOS-Switch# show tacacs	Cisco#show tacacs
ArubaOS-Switch# show authentication	

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
```

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	Cisco
(Requires special configuration on the TACACS server)	(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
```

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	Cisco
Not an available feature	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

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 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	Cisco
(Enabled by default, both globally and per port)	(Not enabled by default)
(if needed) `ArubaOS-Switch(config)# lldp run`	`Cisco(config)#lldp run`
`ArubaOS-Switch# show lldp info remote-device`	`Cisco#show lldp neighbors`
`ArubaOS-Switch# show lldp info remote-device 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

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
```

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	Cisco
(CDP Receive only support enabled by default, both globally and per port)	(Enabled by default, both globally and per port)
(if needed) `ArubaOS-Switch(config)# cdp run`	(if needed) `Cisco(config)#cdp run`
`ArubaOS-Switch# show cdp`	`Cisco#show cdp`
`ArubaOS-Switch# show cdp neighbors`	`Cisco#show cdp neighbors`
`ArubaOS-Switch# show cdp neighbors 5`	`Cisco#show cdp neighbors g1/0/5`
`ArubaOS-Switch# show cdp neighbors 5 detail`	`Cisco#show cdp neighbors g1/0/5 detail`

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
```

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	Cisco
`ArubaOS-Switch(config)# oobm`	`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

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
```

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	Cisco
ArubaOS-Switch(config)# job save-config at 01:00 "copy run tftp 10.0.100.111 ArubaOS-Switch.cfg"	Cisco(config)#file prompt quiet
	Cisco(config)#kron policy-list save-config
	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	Cisco(config)#show scheduler config
ArubaOS-Switch# show 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]

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
```

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.

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	Cisco
ArubaOS-Switch# show interfaces brief	Cisco#show interfaces status
ArubaOS-Switch# show interfaces brief 1	Cisco#show interfaces g1/0/1 status
ArubaOS-Switch# show interfaces 1	Cisco#show interfaces g1/0/1
ArubaOS-Switch(config)# interface 1	Cisco(config)#interface g1/0/1
ArubaOS-Switch(eth-1)# name link-to-core	Cisco(config-if)#description link-to-core
ArubaOS-Switch(eth-1)# speed-duplex auto	Cisco(config-if)#duplex auto
	Cisco(config-if)#speed auto
ArubaOS-Switch(eth-1)# disable	Cisco(config-if)#shutdown
ArubaOS-Switch(eth-1)# enable	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
```

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, 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. 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 Clsco the term is *EtherChannel*.

Interface use	ArubaOS-Switch	Cisco
Non-802.1Q interfaces (such as used for computers or printers)	untagged	access
802.1Q interfaces (such as used for switch-to-switch, switch-to-server, and switch-to-VoIP phones)	tagged	trunk
Aggregated interfaces	trunk	etherchannel

a) Creating and Naming VLANs

ArubaOS-Switch	Cisco
`ArubaOS-Switch(config)# vlan 220`	`Cisco(config)#vlan 220`
`ArubaOS-Switch(vlan-220)# name test`	`Cisco(config-vlan)#name test`
`ArubaOS-Switch# show vlans`	`Cisco#show vlan brief`

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
```

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	Cisco
(tag/untag)	(trunk/access)
ArubaOS-Switch(config)# vlan 220	Cisco(config)#interface g1/0/6
ArubaOS-Switch(vlan-220)# tagged 6	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	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	Cisco#show vlan id 220 Cisco#show vlan id 100 Cisco#show vlan id 1
ArubaOS-Switch# show vlans ports 6 detail	Cisco#show interfaces g1/0/6 switchport
ArubaOS-Switch# show vlans ports 5 detail	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
```

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	Cisco
ArubaOS-Switch(config)# vlan 220	Cisco(config)#interface vlan 220
ArubaOS-Switch(vlan-220)# ip address 10.1.220.1/24	Cisco(config-if)#ip address 10.1.220.2 255.255.255.0
	Cisco(config-if)#no shutdown
ArubaOS-Switch# show ip	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
```

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	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
ArubaOS-Switch# show ip helper-address vlan 220	Cisco#show ip interface vlan 220
ArubaOS-Switch# show dhcp-relay	

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
```

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	Cisco
	`Cisco(config)#vtp mode transparent`
`ArubaOS-Switch(config)# vlan 150 private-vlan primary`	`Cisco(config)#vlan 150`

	`Cisco(config-vlan)#private-vlan primary`
	
	`Cisco(config-vlan)#exit`

`ArubaOS-Switch(config)# vlan 150 private-vlan isolated 151`	`Cisco(config)#vlan 151`

	`Cisco(config-vlan)#private-vlan isolated`
	
	`Cisco(config-vlan)#exit`

`ArubaOS-Switch(config)# vlan 150 private-vlan community 152`	`Cisco(config)#vlan 152`

	`Cisco(config-vlan)#private-vlan community`
	
	`Cisco(config-vlan)#exit`

	`Cisco(config)#vlan 150`
	`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	Cisco(config)#interface g1/0/10
	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	Cisco(config)#interface g1/0/12
	Cisco(config-if)#switchport mode private-vlan host
	Cisco(config-if)#switchport private-vlan host-association 150 151
ArubaOS-Switch(config)# vlan 152 untag 14,15	Cisco(config)#int g1/0/14
	Cisco(config-if)#switchport mode private-vlan host
	Cisco(config-if)#switchport private-vlan host-association 150 152
ArubaOS-Switch(config)# vlan 150 ip address 10.150.1.1/24	Cisco(config)#interface vlan 150
	Cisco(config-if)#ip addr 10.150.3.1 255.255.255.0
	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	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	

b) MVRP

ArubaOS-Switch	Cisco
ArubaOS-Switch(config)# mvrp enable	Cisco(config-if)#feature mvrp
ArubaOS-Switch(config)# interface 1 mvrp enable	
ArubaOS-Switch# show mvrp config	
ArubaOS-Switch# show mvrp state 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]

c) VxLAN

ArubaOS-Switch	Cisco
(example config for HPE 3810)	(example config for Nexus 9000)
ArubaOS-Switch(config)# vxlan enable	Cisco-vtep-1(config)# feature pim
ArubaOS-Switch(config)# vxlan udp 12345	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	Cisco-vtep-1(config)# interface loopback0
ArubaOS-Switch(tunnel-1)# tunnel mode vxlan	Cisco-vtep-1(config-if)# ip pim sparse-mode
ArubaOS-Switch(tunnel-1)# tunnel source 10.222.1.2	Cisco-vtep-1(config-if)# exit
ArubaOS-Switch(tunnel-1)# tunnel destination 10.222.1.1	Cisco-vtep-1(config)# interface e2/1
ArubaOS-Switch(tunnel-1)# exit	Cisco-vtep-1(config-if)# ip pim sparse-mode
ArubaOS-Switch(config)# virtual-network 1 10 virtual-net1	Cisco-vtep-1(config-if)# exit
ArubaOS-Switch(config)# vxlan tunnel 1 overlay-vlan 10	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

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
```

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-value <upper-limit> <lower-limit> action-type {trap | log | trap-log | none }	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 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>} <PORT-NUM> source {<IP-ADDR>|<VLAN-ID>} <PORT-NUM> [payload-size <SIZE>] [num-of-packets <NUM>] [packet-interval <INT>]	Cisco(config)#config- ip-sla-multicast-jitter-oper
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-	Cisco(config)#crypto pki trustpoint name

PROFILE-NAME usage ssh-client subject common-name CN-VALUE	
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.

ArubaOS-Switch pre-std-detect is now off. (It was on in previous versions of the software.)

Cisco autodetects older Cisco pre-standard as well as IEEE-compliant PoE-enabled devices.

ArubaOS-Switch	Cisco
(PoE enabled by default)	(PoE enabled by default) (note, 3750 used for this chapter)
`ArubaOS-Switch# show power-over-ethernet`	
`ArubaOS-Switch# show power-over-ethernet brief`	`Cisco#show power inline`
`ArubaOS-Switch# show power-over-ethernet 5`	`Cisco#show power inline f1/0/5`
`ArubaOS-Switch(config)# interface 5`	`Cisco(config)#interface f1/0/5`
`ArubaOS-Switch(eth-5)# no power-over-ethernet`	`Cisco(config-if)#power inline never`
`ArubaOS-Switch(eth-5)# power-over-ethernet`	`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.
```

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	Cisco
ArubaOS-Switch(config)# vlan 230	Cisco(config)#vlan 230
ArubaOS-Switch(vlan-230)# voice	Cisco(config-vlan)#name voice
	Cisco(config)#interface g1/0/5
	Cisco(config-if)#switchport
ArubaOS-Switch(vlan-230)# vlan 220 ArubaOS-Switch(vlan-220)# untagged 5	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	Cisco(config-if)#switchport voice vlan 230
ArubaOS-Switch# show vlans 230	
ArubaOS-Switch# show vlan ports 5 detail	Cisco#show interfaces g1/0/5 switchport

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
```

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 Cisco , the term is *EtherChannel*. In addition, Cisco Etherchannel has two modes: PAgP (Cisco specific) or LACP. LACP mode is shown in the Cisco configuration examples.

In 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	Cisco
ArubaOS-Switch(config)# trunk 20-23 trk1 lacp	Cisco(config)#interface port-channel 1
ArubaOS-Switch(config)# vlan 220 tagged trk1	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 active
ArubaOS-Switch# show trunks ArubaOS-Switch# show lacp	Cisco#show lacp 1 internal
ArubaOS-Switch# show lacp peer	
ArubaOS-Switch# show lacp peer ArubaOS-Switch# show lacp counters	Cisco#show interfaces etherchannel
ArubaOS-Switch# show vlans 220	Cisco#show vlan name test

ArubaOS-Switch# show vlans ports trk1 detail	

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
```

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	Cisco
ArubaOS-Switch(config)# trunk 19-20 trk1 trunk	Cisco(config)#interface port-channel 1
ArubaOS-Switch(config)# vlan 220 tagged trk1	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
ArubaOS-Switch# show trunks	
	Cisco#show etherchannel 1 summary
	Cisco#show interfaces etherchannel
ArubaOS-Switch# show vlans 220 ArubaOS-Switch# show vlans ports trk1 detail	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
```

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.

- 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	Cisco
`ArubaOS-Switch(config)# spanning-tree`	(Not an available feature)
`ArubaOS-Switch(config)# spanning-tree force-version rstp-operation`	
`ArubaOS-Switch(config)# spanning-tree priority 2`	
`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`	
`ArubaOS-Switch# show spanning-tree`	

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
```

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.

- 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	Cisco
ArubaOS-Switch(config)# spanning-tree	Cisco(config)#spanning-tree mode mst
	Cisco(config)#spanning-tree mst configuration
ArubaOS-Switch(config)# spanning-tree config-name ArubaOS-Switch-Comware-Cisco	Cisco(config-mst)#name ArubaOS-Switch-Comware-Cisco
ArubaOS-Switch(config)# spanning-tree config-revision 1	Cisco(config-mst)#revision 1
ArubaOS-Switch(config)# spanning-tree instance 1 vlan 220	Cisco(config-mst)# instance 1 vlan 220
ArubaOS-Switch(config)# spanning-tree instance 2 vlan 100	Cisco(config-mst)# instance 2 vlan 100
ArubaOS-Switch(config)# spanning-tree instance 3 vlan 240	Cisco(config-mst)# instance 3 vlan 240
ArubaOS-Switch(config)# spanning-tree priority 2	Cisco(config)#spanning-tree mst 0 priority 20480
ArubaOS-Switch(config)# spanning-tree instance 1 priority 3	Cisco(config)#spanning-tree mst 1 priority 16384
ArubaOS-Switch(config)# spanning-tree instance 2 priority 4	Cisco(config)#spanning-tree mst 2 priority 12288
ArubaOS-Switch(config)# spanning-tree instance 3 priority 5	Cisco(config)#spanning-tree mst 3 priority 8192
	Cisco(config)#interface g1/0/9
ArubaOS-Switch(config)# spanning-tree 9 admin-edge-port	Cisco(config-if)#spanning-tree portfast
ArubaOS-Switch(config)# spanning-tree 9 path-cost 10000	Cisco(config-if)#spanning-tree cost 10000
ArubaOS-Switch(config)# spanning-tree 9 priority 10	Cisco(config-if)#spanning-tree port-priority 160

ArubaOS-Switch(config)# spanning-tree instance 1 9 path-cost 10000	Cisco(config-if)#spanning-tree mst 1 cost 10000
ArubaOS-Switch(config)# spanning-tree instance 1 9 priority 10	Cisco(config-if)#spanning-tree mst 1 port-priority 160
ArubaOS-Switch# show spanning-tree	Cisco#show spanning-tree
	Cisco#show spanning-tree mst
ArubaOS-Switch# show spanning-tree mst-config	Cisco#show spanning-tree mst configuration
ArubaOS-Switch# show spanning-tree instance ist	Cisco#show spanning-tree mst 0
ArubaOS-Switch# show spanning-tree instance 1	Cisco#show spanning-tree mst 1

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
```

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.

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*.
- Cisco uses Per-VLAN Spanning Tree Plus (PVST+) as the default STP version and *is enabled by default*.

ArubaOS-Switch	Cisco
`ArubaOS-Switch(config)# spanning-tree mode rapid-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`	`Cisco(config)#spanning-tree vlan 1 priority 20480`
`ArubaOS-Switch(config)# spanning-tree vlan 220 priority 3`	`Cisco(config)#spanning-tree vlan 220 priority 16384`
`ArubaOS-Switch(config)# spanning-tree vlan 100 priority 4`	`Cisco(config)#spanning-tree vlan 100 priority 12288`
`ArubaOS-Switch(config)# spanning-tree vlan 240 priority 5`	`Cisco(config)#spanning-tree vlan 240 priority 8192`
`ArubaOS-Switch(config)# spanning-tree`	

`ArubaOS-Switch# show spanning-tree`	`Cisco#show spanning-tree root`
	
	`Cisco#show spanning-tree summary`

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
```

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	Cisco
ArubaOS-Switch(config)# router rip ArubaOS-Switch(rip)# enable	Cisco(config)#router rip
ArubaOS-Switch(rip)# vlan 220 ip rip	Cisco(config-router)#network 10.1.220.0
	Cisco(config-router)#version 2
ArubaOS-Switch(rip)# redistribute connected	Cisco(config-router)#redistribute connected
ArubaOS-Switch# show ip rip	Cisco#show ip rip database
ArubaOS-Switch# show ip rip interface vlan 220	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
```

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	Cisco
`ArubaOS-Switch(config)# ip router-id 10.0.0.21`	

`ArubaOS-Switch(config)# router ospf`
 	
`ArubaOS-Switch(ospf)# enable`
	`Cisco(config)#router ospf 1`

	`Cisco(config-router)#router-id 10.0.0.41`
`ArubaOS-Switch(ospf)# area 0`	

`ArubaOS-Switch(ospf)# vlan 220`
 	
`ArubaOS-Switch(vlan-220)# ip ospf area 0`
	`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`
	`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
```

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	Cisco
ArubaOS-Switch(config)# router ospf	Cisco(config)#router ospf 1
ArubaOS-Switch(ospf)# area 1	
ArubaOS-Switch(ospf)# area 2	
ArubaOS-Switch(ospf)# vlan 100 ArubaOS-Switch(vlan-100)# ip ospf area 1	Cisco(config-router)#network 10.1.100.0 0.0.0.255 area 1
ArubaOS-Switch(vlan-100)# vlan 230 ArubaOS-Switch(vlan-230)# ip ospf area 2	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
```

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	Cisco
ArubaOS-Switch(ospf)# area 1 stub 11	Cisco(config-router)#area 1 stub

ArubaOS-Switch
ArubaOS-Switch(ospf)# area 1 stub 11
Cisco
Cisco(config-router)#area 1 stub

d) Totally Stubby

ArubaOS-Switch	Cisco
ArubaOS-Switch(ospf)# area 2 stub no-summary 11	Cisco(config-router)#area 2 stub no-summary
ArubaOS-Switch(config)# vlan 230	Cisco(config-if)#interface vlan 230
ArubaOS-Switch(vlan-230)# ip 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
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	Cisco
ArubaOS-Switch# show ip ospf interface	Cisco#show ip ospf interface brief
ArubaOS-Switch# show ip ospf neighbor	Cisco#show ip ospf neighbor
ArubaOS-Switch# show ip ospf link-state	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
```

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	Cisco
ArubaOS-Switch(config)# router bgp 64502	Cisco(config)#router bgp 64504
ArubaOS-Switch(bgp)# bgp router-id 10.0.0.2	Cisco(config-router)#bgp router-id 10.0.0.4
ArubaOS-Switch(bgp)# neighbor 10.0.101.31 remote-as 64503	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	Cisco(config-router)#redistribute connected
ArubaOS-Switch(bgp)# redistribute static	
ArubaOS-Switch(bgp)# enable	
ArubaOS-Switch(bgp)# network 10.0.221.0/24	Cisco(config-router)#network 10.0.241.0 mask 255.255.255.0
ArubaOS-Switch# show ip bgp summary	Cisco#show ip bgp summary

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
```

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	Cisco
iBGP router:	iBGP router:
ArubaOS-Switch-2(config)# router bgp 64502	Cisco-2(config)#router bgp 64504
ArubaOS-Switch-2(bgp)# bgp router-id 10.0.0.12	Cisco-2(config-router)#bgp router-id 10.0.0.14
ArubaOS-Switch-2(bgp)# neighbor 10.0.112.254 remote-as 64502	Cisco-2(config-router)#neighbor 10.0.114.254 remote-as 64504
ArubaOS-Switch-2(bgp)# redistribute connected	Cisco-2(config-router)#redistribute connected
ArubaOS-Switch-2(bgp)# enable	
ArubaOS-Switch-2(bgp)# network 10.0.222.0/24	Cisco-2(config-router)#network 10.0.242.0 mask 255.255.255.0
ArubaOS-Switch-2# show ip bgp summary	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.
ArubaOS-Switch(config)# router bgp 64502	Cisco(config)#router bgp 64504
ArubaOS-Switch(bgp)# neighbor 10.0.112.1 remote-as 64502	Cisco(config-router)#neighbor 10.0.114.1 remote-as 64504
ArubaOS-Switch(bgp)# neighbor 10.0.112.1 next-hop-self	Cisco(config-router)#neighbor 10.0.114.1 next-hop-self
ArubaOS-Switch# show ip bgp summary	Cisco#show ip bgp summary

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
```

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	Cisco
ArubaOS-Switch(config)# router vrrp ArubaOS-Switch(vrrp)# ipv4 enable	
ArubaOS-Switch(vrrp)# 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	Cisco(config-if)#vrrp 100 ip 10.1.100.1
ArubaOS-Switch(vlan-220-vrid-220)# priority 254	Cisco(config-if)#vrrp 100 priority 100
ArubaOS-Switch(vlan-220-vrid-220)# enable	
ArubaOS-Switch# show vrrp	Cisco#show vrrp
	Cisco#show vrrp brief
ArubaOS-Switch# show vrrp vlan 220	Cisco#show vrrp interface vlan 100

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
```

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).

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.
```

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	Cisco
`ArubaOS-Switch(config)# ip access-list standard 1`	`Cisco(config)#ip access-list standard 1`
`ArubaOS-Switch(config-std-nacl)# permit 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`	`Cisco(config)#ip access-list standard std_acl`
`ArubaOS-Switch(config-std-nacl)# permit 10.0.100.111/32`	`Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0`

Extended/Advanced

ArubaOS-Switch	Cisco
ArubaOS-Switch(config)# ip access-list extended 100	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	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	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	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	

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 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	Cisco
ArubaOS-Switch(config)# ip access-list standard 1	Cisco(config)#ip access-list standard 1
ArubaOS-Switch(config-std-nacl)# permit 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	Cisco(config)#ip access-list standard std_acl
ArubaOS-Switch(config-std-nacl)# permit 10.0.100.111/32	Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0
ArubaOS-Switch(config-std-nacl)# vlan 220	Cisco(config-std-nacl)#interface vlan 220
ArubaOS-Switch(vlan-220)# ip access-group 1 in	Cisco(config-if)#ip access-group 1 in
ArubaOS-Switch(config)# vlan 100	Cisco(config)#interface vlan 100
ArubaOS-Switch(vlan-100)# ip access-group std_acl in	Cisco(config-if)#ip access-group std_acl in

Extended or Advanced ACL

ArubaOS-Switch	Cisco
ArubaOS-Switch(config)# ip access-list extended 100	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	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	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	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	Cisco(config)#interface vlan 220
ArubaOS-Switch(vlan-220)# ip access-group 100 in	Cisco(config-if)#ip access-group 100 in
ArubaOS-Switch(vlan-220)# vlan 100	Cisco(config-if)#interface vlan 100
ArubaOS-Switch(vlan-100)# ip access-group ext_acl in	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
```

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 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	Cisco
ArubaOS-Switch(config)# ip access-list standard 10	Step - 1
ArubaOS-Switch(config-std-nacl)# deny 10.1.220.102 0.0.0.0	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	Cisco(config-access-map)#match ip address 10
ArubaOS-Switch(vlan-220)# ip access-group 10 vlan	Cisco(config-access-map)#action drop
	Step - 3
	Cisco(config)#vlan filter vacl_1 vlan-list 220

Extended or Advanced ACL

ArubaOS-Switch	Cisco
ArubaOS-Switch(config)# ip access-list extended 110	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
```

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 Cisco, a Port ACL access-controls traffic entering a Layer 2 interface.

Standard or Basic ACL

ArubaOS-Switch	Cisco
ArubaOS-Switch(config)# ip access-list standard 11	Cisco(config)#ip access-list standard 11
ArubaOS-Switch(config-std-nacl)# permit 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_pacl	Cisco(config)#ip access-list standard std_pacl
ArubaOS-Switch(config-std-nacl)# permit 10.0.100.111/32	Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0
ArubaOS-Switch(config)# interface 4	Cisco(config)#interface g1/0/4
ArubaOS-Switch(eth-4)# ip access-group 11 in	Cisco(config-if)#ip access-group 11 in
ArubaOS-Switch(eth-4)# ip access-group std_pacl in	Cisco(config-if)#ip access-group std_pacl in

Extended or Advanced ACL

ArubaOS-Switch	Cisco
ArubaOS-Switch(config)# ip access-list extended 111	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	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	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	Cisco(config-ext-nacl)#deny ip 10.1.220.0 255.255.255.0 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)# interface 4	Cisco(config)#interface g1/0/4
ArubaOS-Switch(eth-4)# ip access-group 111 in	Cisco(config-if)#ip access-group 121 in
ArubaOS-Switch(eth-4)# ip access-group ext_pacl in	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
```

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, 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	Cisco
QoS default	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 SVI
Marking	Configured primarily on a global basis. Some configuration options can be set globally and some also set at VLAN or port	Configured per port or on SVI
Queue Scheduling	Configured per port	Configured per port or on SVI

a) QoS

ArubaOS-Switch	Cisco
	Cisco(config)#mls qos
	Cisco(config)#interface g1/0/5
	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	Cisco(config)#interface g1/0/5
ArubaOS-Switch(eth-5)# qos priority 6	Cisco(config-if)#mls qos cos 6
ArubaOS-Switch(config)# vlan 230	
ArubaOS-Switch(vlan-230)# qos priority 6	
ArubaOS-Switch# show 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.
```

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	Cisco
ingress	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
ArubaOS-Switch(config)# interface 8	Cisco(config)#interface g1/0/8
ArubaOS-Switch(eth-8)# rate-limit all out kbps 10000	Cisco(config-if)#srr-queue bandwidth limit 10

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
```

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	Cisco
ArubaOS-Switch(config)# ip multicast-routing	Cisco(config)#ip multicast-routing distributed
ArubaOS-Switch(config)# router pim ArubaOS-Switch(pim)# enable	
ArubaOS-Switch(pim)# vlan 220	Cisco(config)#interface vlan 220
ArubaOS-Switch(vlan-220)# ip pim-dense	Cisco(config-if)#ip pim dense-mode
ArubaOS-Switch# show ip pim ?	Cisco#show ip pim ?
ArubaOS-Switch# show ip mroute ?	Cisco#show ip mroute ?

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>
```

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	Cisco
ArubaOS-Switch(config)# ip multicast-routing	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	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	Cisco(config)#ip pim rp-address 10.1.220.1
ArubaOS-Switch(pim)# rp-candidate source-ip-vlan 220	Cisco(config)#ip pim rp-candidate vlan 220
ArubaOS-Switch(pim)# bsr-candidate source-ip-vlan 220	Cisco(config)#ip pim bsr-candidate vlan 220
ArubaOS-Switch# show ip pim ?	Cisco#show ip pim ?
ArubaOS-Switch# show ip mroute ?	Cisco#show ip mroute ?

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>
```

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	Cisco
ArubaOS-Switch(vlan-220)# ip igmp	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
```

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	Cisco
ArubaOS-Switch(config)# interface 17	Cisco(config)#interface g1/0/17
ArubaOS-Switch(eth-17)# link-keepalive	Cisco(config-if)#udld port
ArubaOS-Switch# show link-keepalive	Cisco#show udld g1/0/17
ArubaOS-Switch# show link-keepalive 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
```

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	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

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"
```

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	Cisco
ArubaOS-Switch(config)# loop-protect 17 receiver-action send-disable	Cisco(config)#interface g1/0/17 Cisco(config-if)#spanning-tree guard loop

ArubaOS-Switch
ArubaOS-Switch(config)# loop-protect 17 receiver-action send-disable
Cisco
Cisco(config)#interface g1/0/17 Cisco(config-if)#spanning-tree guard loop

d) Root Guard

ArubaOS-Switch	Cisco
ArubaOS-Switch(config)# spanning-tree 17 root-guard	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
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	Cisco
ArubaOS-Switch(config)# 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
ArubaOS-Switch(config)# dhcp-snooping vlan 220	Cisco(config)#ip dhcp snooping vlan 220
ArubaOS-Switch(config)# dhcp-snooping trust 1	Cisco(config)#interface g1/0/6 Cisco(config-if)#ip dhcp snooping trust
ArubaOS-Switch# show dhcp-snooping	Cisco#show ip dhcp snooping
	Cisco#show ip dhcp snooping database
ArubaOS-Switch# show dhcp-snooping stats	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

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
```

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	Cisco
ArubaOS-Switch(config)# dhcp-snooping	Cisco(config)#ip dhcp snooping
ArubaOS-Switch(config)# arp-protect	
ArubaOS-Switch(config)# arp-protect vlan 220	Cisco(config)#ip arp inspection vlan 220
ArubaOS-Switch(config)# arp-protect trust 1	Cisco(config)#interface g1/0/6
	Cisco(config-if)#ip arp inspection trust
ArubaOS-Switch# show arp-protect	Cisco#show ip arp inspection
ArubaOS-Switch# show arp-protect statistics 220	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

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
```

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.)

Cisco do not support this exact feature. However, their Address Resolution Protocol (ARP) commands provide rate limiting capabilities for incoming ARP packets.

ArubaOS-Switch	Cisco
	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`	`Cisco(config-if)#interface g1/0/20`
`ArubaOS-Switch(config)# filter connection-rate 7 notify-only`	`Cisco(config-if)#ip arp inspection limit rate 100`
`ArubaOS-Switch(config)# filter connection-rate 10 block`	
`ArubaOS-Switch(config)# filter connection-rate 17 throttle`	
`ArubaOS-Switch# show connection-rate-filter`	`Cisco#show ip arp inspection interfaces`

ArubaOS-Switch

```
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
```

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	Cisco
ArubaOS-Switch(config)# radius-server host 10.0.100.111 key password	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	Cisco(config)#dot1x system-auth-control
ArubaOS-Switch(config)# aaa port-access authenticator 14 unauth-vid 99	

ArubaOS-Switch(config)# aaa port-access authenticator 14 client-limit 1	Cisco(config)#interface g1/0/14
	Cisco(config-if)#switchport mode access
ArubaOS-Switch(config)# aaa port-access authenticator active	Cisco(config-if)#dot1x pae authenticator
	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 authenticator	Cisco#show dot1x all summary
ArubaOS-Switch# show port-access authenticator vlan	
ArubaOS-Switch# show vlans ports 14 detail	Cisco#show dot1x interface g1/0/14 details
ArubaOS-Switch# show vlans 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

b) MAC Authentication

ArubaOS-Switch	Cisco
ArubaOS-Switch(config)# radius-server host 10.0.100.111 key password	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	Cisco(config)#interface g1/0/16
	Cisco(config-if)#switchport mode access
ArubaOS-Switch(config)# aaa port-access mac-based 16 unauth-vid 99	Cisco(config-if)#dot1x pae authenticator
	Cisco(config-if)#mab
	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	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	

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
```

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	Cisco
ArubaOS-Switch(config)# radius-server host 10.0.100.111 key password	(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	Cisco(config)#aaa new-model
ArubaOS-Switch(config)# aaa port-access web-based 18 unauth-vid 99	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	Cisco(config)#ip device tracking
	Cisco(config)#ip admission name web-auth-rule1 proxy http 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 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 pae authenticator
	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
ArubaOS-Switch# show port-access web-based	Cisco#show ip admission cache
ArubaOS-Switch# show port-access web-based clients	
ArubaOS-Switch# show port-access web-based config 18	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
```

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	Cisco
(Note: ArubaOS-Switch manual indicates to configure destination then source)	(Note: Cisco manual indicates to configure source then destination)
	`Cisco(config)#monitor session 1 source interface g1/0/6 both`
`ArubaOS-Switch(config)# mirror 1 port 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`	`Cisco#show monitor`
`ArubaOS-Switch# show monitor 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         -
```

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 Cisco, mirrored traffic traverses the same Layer 2 network (subnet).

ArubaOS-Switch	Cisco
(switch where analyzer is connected)	(switch with traffic of interest)
`ArubaOS-Switch(config)# mirror endpoint ip 10.0.222.254 7922 10.0.111.21 port 4`	`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(config)# monitor session 1 source interface f1/0/1`
	`Cisco2(config)# monitor session 1 destination remote vlan 950`
`ArubaOS-Switch# show monitor`	`Cisco2#show monitor`
`ArubaOS-Switch# show monitor endpoint`	`Cisco2#show monitor session 1 detail`
(switch with traffic of interest)	(switch where analyzer is connected)
`ArubaOS-Switch2(config)# mirror endpoint ip 10.0.222.254 7922 10.0.111.21`	`Cisco(config)#vlan 950`
`ArubaOS-Switch2(config)# interface 1 monitor all both mirror 1`	`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 remote vlan 950`
	`Cisco(config)#monitor session 1 destination interface g1/0/4 encapsulation replicate`
`ArubaOS-Switch2# show monitor 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         -
```

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.

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
```

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 CLI Commands in ArubaOS-Switch Software

This appendix shows display commands added to ArubaOS-Switch software.

Included are related ArubaOS-Switch software commands. Refer to the latest release notes for your switch product to determine which commands are supported.

HPE Networking has added CLI commands into the ArubaOS-Switch software in a phased manner over several releases to help network management staff learn to use the ArubaOS-Switch software CLI with a minimum of effort.

Refer to the latest HP Switch Software – CLI Commands in the ArubaOS-Switch Software reference guide.

ArubaOS-Switch K.16.03.0003 was used for this section.

a) Fundamental Commands

ArubaOS-Switch commands
copy startup-config tftp <ip-address> <file name>
clock set <HH:MM:SS> <MM/DD/YYYY>
clock summer-time
clock timezone
aaa accounting commands
aaa authorization commands radius
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
copy
erase startup-config
flow-control
console inactivity-timer
exit
boot
erase startup
copy tftp startup-config
end
write memory
reload at
reload after
terminal length
set authentication password
console baud-rate
startup-default config <config file name>
hostname
configure
telnet
telnet-server
console terminal
no
Sys-debug ip fib blackhole
Sys-debug ipv6 fib blackhole
Sys-debug destination logging

Sys-debug destination buffer
Ipv6 route <network/subnetmask> blackhole logging
Ip route <network/subnetmask> blackhole logging
Access-list logtimer <5-300>
Sys-debug acl
Sys-debug destination buffer
Sys-debug destination logging
vsf sequence-reboot {primary | secondary}
vsf domain 20
vsf lldp-mad ipv4 10.1.1.1 v2c public
vsf member 4 link 1 name NAME-STR
vsf member 4 link 1 all start-disabled
vsf member 4 link 1 all
vsf member 4 link 1
vsf member 4 priority 255
vsf member 4 remove reboot
vsf member 4 remove
vsf member 4 shutdown
vsf member 4 type <jnum> mac-address <mac-ad>
vsf member 4 type <jnum>
vsf port-speed 1g
vsf port-speed 10g
vsf vlan-mad 707

b) Display Commands

ArubaOS-Switch commands
show arp

show arp-protection
show arp-protection statistics
show arp
show flash
show time show system information
show alias
show interface <port>
show interface <interface>
show cpu
No equivalent ArubaOS-Switch software command
show running-configuration
show running-configuration
No equivalent ArubaOS-Switch software command
show running-configuration
show debug
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
show dhcp-relay
show dhcp-snooping
show dhcp-snooping
show dhcp-snooping binding
show dhcp-snooping statistics
show dhcp-snooping
show tech
show ip dns
No equivalent ArubaOS-Switch software command
show ip dns
show port-access authenticator config
show port-access authenticator config
show port-access authenticator session counters
show port-access authenticator statistics
show system temperature
show system fans
show secure-mode
show gvrp
show gvrp
show gvrp
show gvrp
show gvrp
No equivalent ArubaOS-Switch software command
show history
show tacacs
show ip igmp groups
show ip igmp vlan <vid>
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
show ip igmp vlan <vid>
show ip igmp vlan <vid>
No equivalent ArubaOS-Switch software command
show ip igmp vlan <vid>
No equivalent ArubaOS-Switch software command
show ip igmp vlan <vid>
No equivalent ArubaOS-Switch software command
show ip igmp vlan <vid>

show ip igmp vlan <vid>
show interface
show interfaces brief
show interfaces brief
show ip aspath-list
show dhcp-snooping bindings
show ip community-list
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
show ip prefix-list
show lacp local
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
show lldp info remote-device
show lldp info remote
show lldp info remote
show lldp stats
show lldp stats
show lldp stats
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
show logging
No equivalent ArubaOS-Switch software command
show mac-address
show system information
No equivalent ArubaOS-Switch software command
show port-access mac-based
show port-access mac-based
show system information
show uplink-failure-detection
show vsf vlan-mad
Show vsf
Show vsf detail
Show vsf link detail
Show vsf link utilization
Show vsf lldp-mad parameters
Show vsf lldp-mad status
Show vsf member <member id> link detail
Show vsf member <member id> link <link id> detail

Show vsf member <member id> link <link id> load-balance mac <source mac> <dest mac> inbound-port <port num>
Show vsf topology change-history
Show vsf topology detail
Show vsf trunk-designated-forwarder member <member id>
Show vsf trunk-designated-forwarder
Show vsf vlan-mad
show ip pim interface <interface>
No equivalent ArubaOS-Switch software command
show ip pim neighbor
show ip pim neighbor
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
show power-over-ethernet brief
show power-over-ethernet brief
show power-over-ethernet brief
show power-over-ethernet brief
show system power-supply
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
show system power-supply
show system power-supply
show system power-supply
show crypto host-public-key show ip host-public-key
show ip client-public-key
show radius show radius host show accoutning
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
show rmon statistics
show route-map
show config
show config
show reload <after|at>
show sflow agent
sh sflow <receiver table number> sampling-polling
show snmpv3 community
show snmpv3 group
show snmpv3 engineid
show snmpv3 group
No equivalent ArubaOS-Switch software command
show system information
show snmp-server traps
show snmpv3 user

No equivalent ArubaOS-Switch software command
show ip ssh
No equivalent ArubaOS-Switch software command
show ip ssh
show ip ssh
show ip ssh
No equivalent ArubaOS-Switch software command
show spanning-tree
show spanning-tree detail show spanning-tree <port> detail
show spanning-tree detail
show spanning-tree detail
show spanning-tree detail
show spanning-tree config show spanning-tree <port-list> detail
show spanning-tree config show spanning-tree <port-list> detail
show spanning-tree config show spanning-tree <port-list> detail
show spanning-tree config show spanning-tree <port-list> detail
show spanning-tree config show spanning-tree <port-list> detail
show spanning-tree config show spanning-tree <port-list> detail
show spanning-tree config show spanning-tree <port-list> detail
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
show spanning-tree
show spanning-tree
show spanning-tree
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
No equivalent ArubaOS-Switch software command
show spanning-tree mst-config
show spanning-tree instance <instance-id> show spanning-tree detail
show redundancy
show boot-history
No equivalent ArubaOS-Switch software command
show interface transceiver detail
show interface transceiver [<port>|detail]
show interface transceiver [<port>|detail]
show interface transceiver [<port>|detail]
show ip source-lockdown bindings
show vlan
show vrrp
show vrrp <interface-type> vrid <virtual routerid>
show vrrp statistics
show vrrp statistics global
show vrrp

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

♥ 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 and Cisco IOS CLI Reference Guide

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