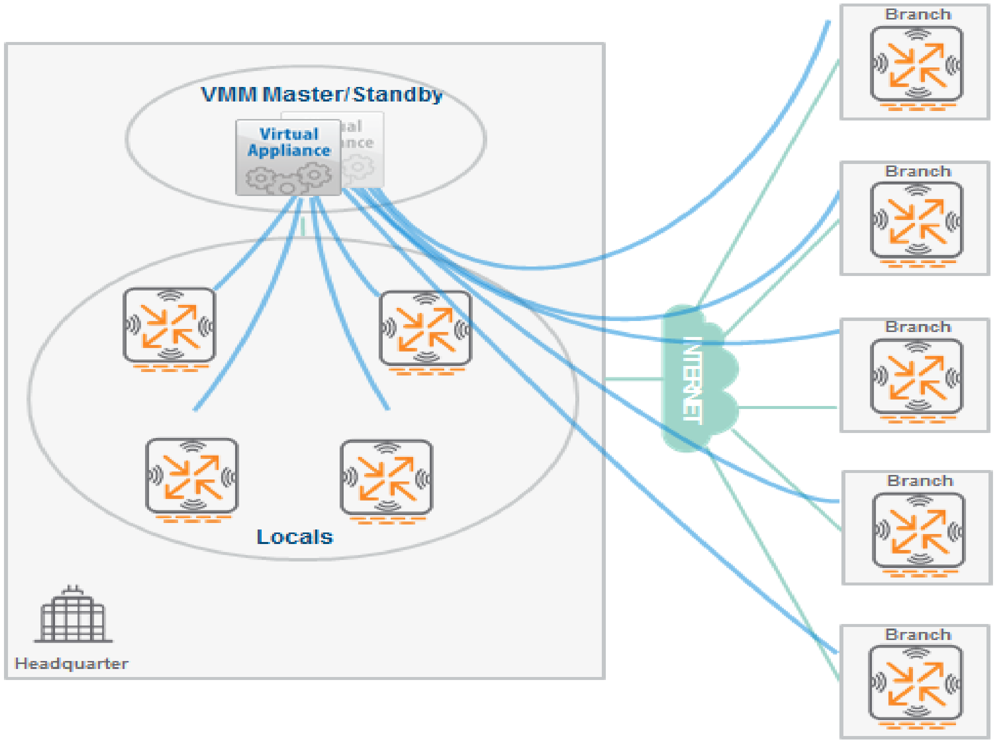
基于 AOS8.X 下的 VMM+ VPNC+ Branch MD 的场景化配置

1. 场景需求：



在具有多分支的 **AOS8.X** 部署架构中，大多数客户使用的 **Mobility Master** 控制器是基于虚拟机部署的（也叫作 **Virtual Mobility Master----**简称 **VMM**），而此时 **VMM** 控制器由于采用的是基于 **X86** 的硬件架构，所以并没有专用的硬件 **IPSec** 加解密芯片来更好地处理加密数据，当多个分支的 **Branch MD** 控制器将 **IPSec** 隧道直接终结在 **VMM** 控制器上时，很容易导致 **VMM** 控制器需要处理大量的 **IPSec** 加密数据，依赖传统的 **X86** 硬件架构，很容易产生性能瓶颈，从而影响数据传输的效率。

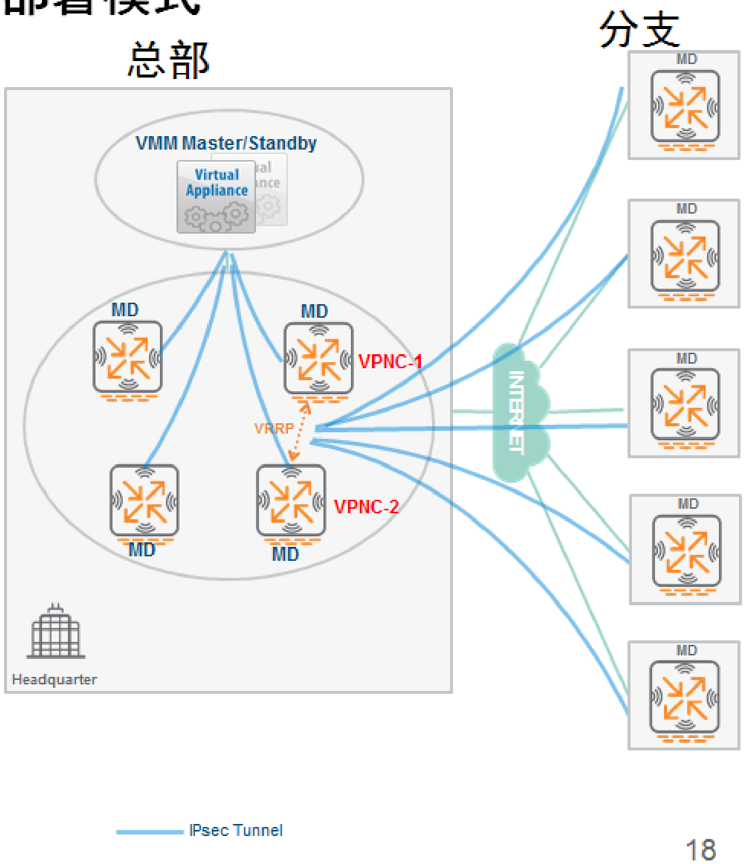
2. 解决方法：

解决这个问题的方法是在靠近 **VMM** 控制器的数据中心，部署基于硬件型号的 **MD** 控制器（角色也叫作 **VPN Concentrator--- VPN** 集中器，简称 **VPNC**），该 **VPNC** 可以兼做本地无线控制器来终结 **AP**，同时将多个分支的 **Branch MD** 控制器的 **IPSec** 隧道由原来指向 **VMM**，全部转为终结在硬件 **VPNC** 控制器上，然后由硬件 **VPNC** 控制器仅建立一个 **IPSec** 隧道到 **VMM** 控制器，从而减轻了 **VMM** 控制器需要终结多个 **IPSec** 隧道的性能瓶颈，而硬件 **VPNC** 控制器会采用专用的硬件芯片来游刃有余地处理 **IPSec** 加密数据。

解决办法：采用8.x – 增强的Branch MD部署模式

总部部署的VPN Concentrator（VPNC）

1. VMM不终结分支MD的IPsec隧道
2. 一个或者一对硬件MD作为VPNC，用于终结 Branch MD的IPSec隧道
3. 消除在VMM上进行加解密服务的性能瓶颈
4. 从VPNC到VMM，仅有一条IPSec隧道
5. 8.x的Branch MD 和VPNC，其实都是普通的MD控制器，只是扮演的角色不同



aruba
a Hewlett Packard Enterprise company

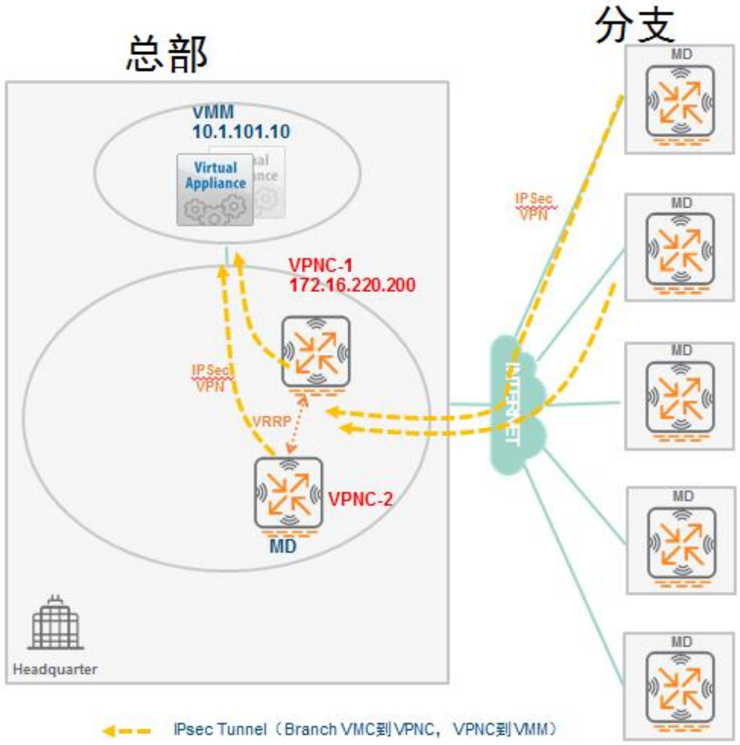
3. 部署拓扑图：

我们在总部设计 **1-2** 台 **MD** 控制器，采用硬件型号例如 **AC72xx** 系列控制器，来扮演 **VPN** 聚合器（**VPNC**）的功能，将所有分支 **Branch MD** 控制器的 **IPSec** 隧道进行终结，然后 **VPN** 聚合器（**VPNC**）采用单一的 **IPSec** 隧道和 **VMM** 进行通讯，这样 **VPNC** 就能加速 **VMM** 和 **Branch MD** 之间的加密数据传输，也规避了性能的瓶颈。

总部设计VPN Concentrator(VPNC)拓扑图

VMM Management MAC Address is 00:0C:29:37:E5:44

VPNC-1 Management MAC Address is 00:0B:86:9A:D5:D7



Branch-MD
10.1.102.51

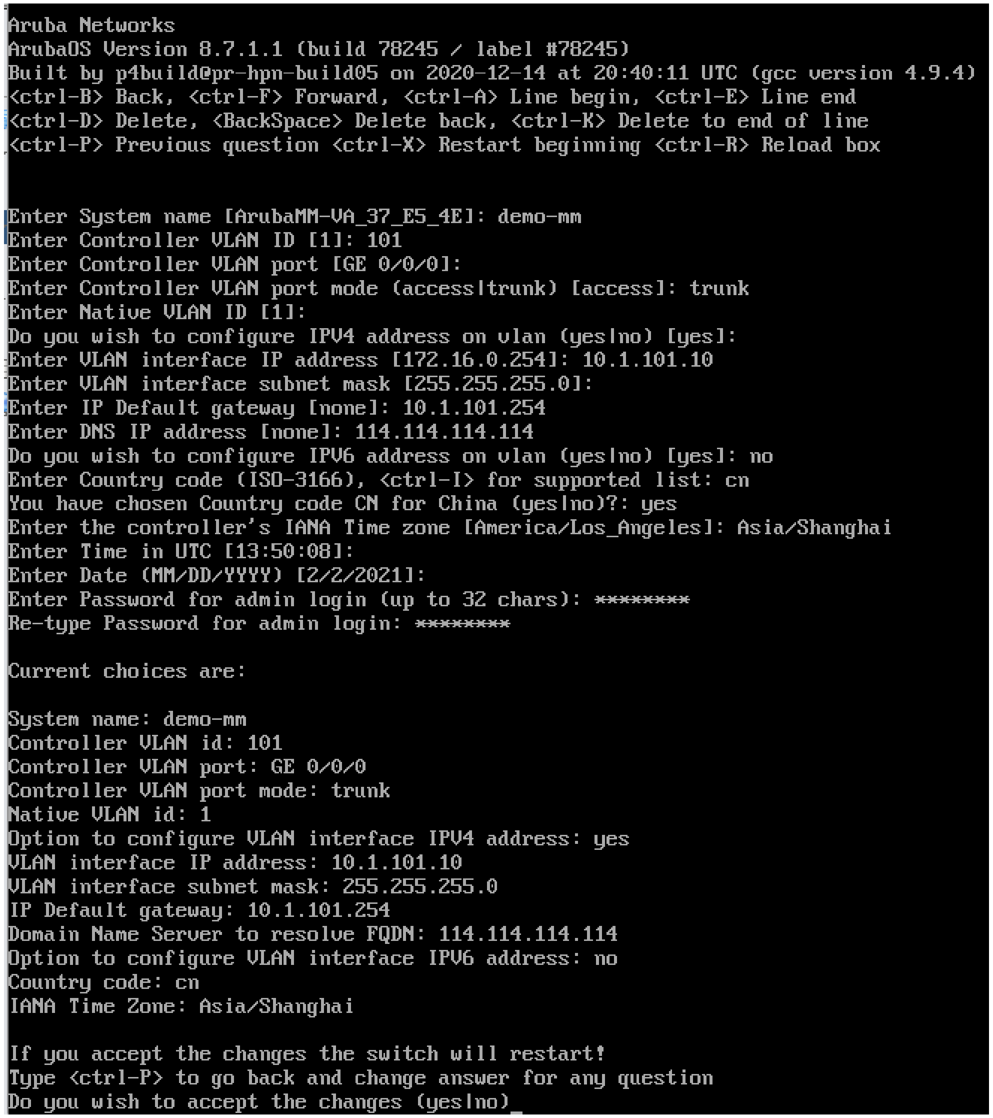
Branch-MD Management MAC Address is 00:0C:29:96:81:A9

4. 相关的配置：

1） VMM， VPNC 和 Branch-MD 全部采用基于初始化向导方式来完成 部署

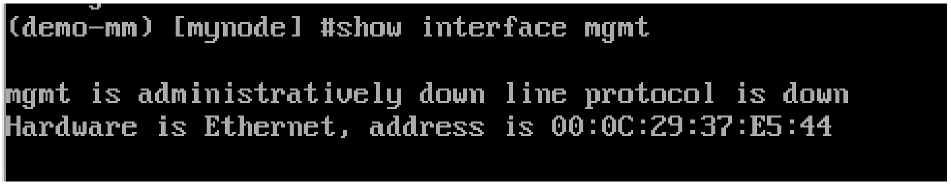
Step1----和常规场景下的 VMM 部署一样，完成初始化即可

注意	本环境下，VMM 采用 GE 0/0/0 口上联，并采用 Trunk 模式，Controller VLAN ID=101， Native VLAN ID =1

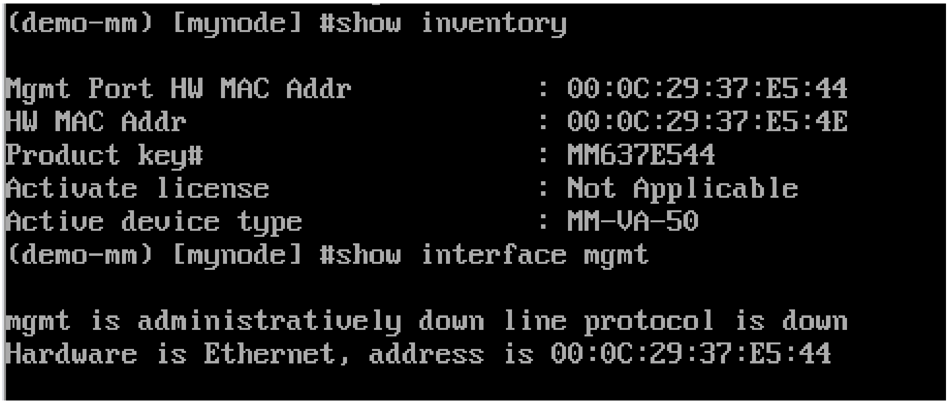


```
Aruba Networks
ArubaOS Version 8.7.1.1 (build 78245 / label #78245)
Built by p4build@pr-hpn-build05 on 2020-12-14 at 20:40:11 UTC (gcc version 4.9.4)
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box


Enter System name [ArubaMM-VA_37_E5_4E]: demo-mm
Enter Controller VLAN ID [1]: 101
Enter Controller VLAN port [GE 0/0/0]:
Enter Controller VLAN port mode (access|trunk) [access]: trunk
Enter Native VLAN ID [1]:
Do you wish to configure IPV4 address on vlan (yes|no) [yes]:
Enter VLAN interface IP address [172.16.0.254]: 10.1.101.10
Enter VLAN interface subnet mask [255.255.255.0]:
Enter IP Default gateway [none]: 10.1.101.254
Enter DNS IP address [none]: 114.114.114.114
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
Enter Country code (ISO-3166), <ctrl-I> for supported list: cn
You have chosen Country code CN for China (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]: Asia/Shanghai
Enter Time in UTC [13:50:08]:
Enter Date (MM/DD/YYYY) [2/2/2021]:
Enter Password for admin login (up to 32 chars): ********
Re-type Password for admin login: ********

Current choices are:

System name: demo-mm
Controller VLAN id: 101
Controller VLAN port: GE 0/0/0
Controller VLAN port mode: trunk
Native VLAN id: 1
Option to configure VLAN interface IPV4 address: yes
VLAN interface IP address: 10.1.101.10
VLAN interface subnet mask: 255.255.255.0
IP Default gateway: 10.1.101.254
Domain Name Server to resolve FQDN: 114.114.114.114
Option to configure VLAN interface IPV6 address: no
Country code: cn
IANA Time Zone: Asia/Shanghai

If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no)_
```

查看并记录 VMM 的 Management MAC Address （也就是 Mgmt Port HW MAC Addr），后面的 VPNC 初始化配置中会使用到。



```
(demo-mm) [mynode] #show interface mgmt

mgmt is administratively down line protocol is down
Hardware is Ethernet, address is 00:0C:29:37:E5:44
```



```
(demo-mm) [mynode] #show inventory

Mgmt Port HW MAC Addr           : 00:0C:29:37:E5:44
HW MAC Addr                     : 00:0C:29:37:E5:4E
Product key#                    : MM637E544
Activate license                : Not Applicable
Active device type              : MM-VA-50
(demo-mm) [mynode] #show interface mgmt

mgmt is administratively down line protocol is down
Hardware is Ethernet, address is 00:0C:29:37:E5:44
```

注意

针对 VMM 和 VMC，这里的 Mgmt Port HW MAC Addr (也就是我们需要的 Management MAC Address) 和 HW MAC Addr 是不一致的，我们需要使用的是 Mgmt Port HW MAC Addr。

Step2----VPNC 的初始化，和常规的 MD 初始化不同，需要指定该 MD 为 VPNC 角色。

注意	本环境中，我们演示的仅部署一台 VPNC-1，它采用 GE 0/0/15 口上联，并采用 Access 模式，Controller VLAN ID=23(初始化的时候也叫作 Uplink VLAN ID)。 如果需要部署两台 VPNC 的话，我们还需要在两台 VPNC 上启用 VRRP，同时将 172.16.220.200 地址设计为 VRRP 的 VIP。

```
Auto-provisioning is in progress. It requires DHCP and Activate servers

Choose one of the following options to override or debug auto-provisioning...

    'enable-debug'     : Enable auto-provisioning debug logs

    'disable-debug'    : Disable auto-provisioning debug logs

    'mini-setup'       : Start mini setup dialog. Provides minimal customization and requires DHCP server

    'full-setup'       : Start full setup dialog. Provides full customization

    'static-activate'  : Provides customization for static or PPPOE ip assignment. Uses activate for master information


Enter Option (partial string is acceptable): full-setup   （我们仍然选择 full-setup 模式）

Are you sure that you want to stop auto-provisioning and start full setup dialog? (yes/no): yes



***************** Welcome to the Aruba7010 setup dialog *****************

This dialog will help you to set the basic configuration for the switch.

These settings, except for the Country Code, can later be changed from the
```

```
Command Line Interface or Graphical User Interface.


Commands: <Enter> Submit input or use [default value], <ctrl-I> Help
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box


Enter System name [Aruba7010_9A_D5_D7]: demo-vpnc
Enter Switch Role (standalone|md) [md]:
Enter IP type to terminate IPSec tunnel or secured websocket connection (ipv4|ipv6) [ipv4]:
Enter Master switch IP address/FQDN or ACP IP address/FQDN: 10.1.101.10
Enter Master switch Type? (MM|ACP) [MM]:
Is this a VPN concentrator for managed device to reach Master switch (yes|no) [no]: yes    （这里非常重要，我们选择 yes）
Enter IPSec Pre-shared Key: ********
Re-enter IPSec Pre-shared Key: ********
Enter Master switch MAC address: 00:0C:29:37:E5:44      （这里就是前面我们看到的 VMM 的 Mgmt Port HW MAC Addr）
Enter Redundant Master switch MAC address [none]:         （如果有第二台备用 VMM，请输入它的 Mgmt Port HW MAC Addr ）
```

```
Do you want to enable L3 Redundancy (yes|no) [no]: no

Enter Uplink Vlan ID [1]: 23

Enter Uplink port [GE 0/0/0]: GE 0/0/15

Enter Uplink port mode (access|trunk) [access]:

Enter Uplink Vlan IP assignment method (dhcp|static|pppoe) [static]:

Enter Uplink Vlan Static IP address [172.16.0.254]: 172.16.220.200

Enter Uplink Vlan Static IP netmask [255.255.255.0]: 255.255.255.128

Enter IP default gateway [none]: 172.16.220.254

Enter DNS IP address [none]: 114.114.114.114

Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no

Do you want to configure dynamic port-channel (yes|no) [no]: no

Enter Country code (ISO-3166), <ctrl-I> for supported list: cn

You have chosen Country code CN for China (yes|no)?: yes

Enter the controller's IANA Time zone [America/Los_Angeles]: Asia/Shanghai

Enter Time in UTC [07:42:56]:

Enter Date (MM/DD/YYYY) [2/4/2021]:

Do you want to create admin account (yes|no) [yes]:
```

```
Enter Password for admin login (up to 32 chars): ********

Re-type Password for admin login: ********



Current choices are:

System name: demo-vpnc

Switch Role: md

IP type to terminate IPSec tunnel or secured websocket connection: ipv4

Master switch IP address or FQDN: 10.1.101.10

Is this VPN concentrator: yes

Master switch MAC address: 00:0C:29:37:E5:44

Vlan id for uplink interface: 23

Uplink port: GE 0/0/15

Uplink port mode: access

Uplink Vlan IP assignment method: static

Uplink Vlan static IP Address: 172.16.220.200

Uplink Vlan static IP net-mask: 255.255.255.128

Uplink Vlan IP default gateway: 172.16.220.254
```

```
Domain Name Server to resolve FQDN: 114.114.114.114

Option to configure VLAN interface IPV6 address: no

Country code: cn

IANA Time Zone: Asia/Shanghai

Admin account created: yes

Note: These settings require IP-Based-PSK configuration on Master switch

If you accept the changes the switch will restart!

Type <ctrl-P> to go back and change answer for any question

Do you wish to accept the changes (yes|no)    yes
```

等 VPNC 重启完成后，接着查看并记录 VPNC 的 Management MAC Address，为了允许 VPNC 和 VMM 之间的通讯，这个 VPNC 的 Management MAC Address 地址是需要的，会在后续的 VMM 上的 local-peer-mac 命令中使用到。

```
(demo-vpnc) #show interface mgmt

mgmt is up line protocol is down

Hardware is Ethernet, address is 00:0B:86:9A:D5:D7



(demo-vpnc) #show inventory
```

```
Supervisor Card slot          : 0

System Serial#              : CG0003800 (Date:08/28/14)

CPU Card Serial#              : AE31003088 (Date:08/05/14)

CPU Card Assembly#            : 2010184C

CPU Card Revision             : (Rev:06.00)

SC Model#                   : Aruba7010

HW MAC Addr                   : 00:0b:86:9a:d5:d7   to   00:0b:86:9a:d5:f6

CPLD Version                 : (Rev: 12.8)

PoE Firmware Version          : 1.7.0 (Build: 4)

Power Supply                 : Present

                        : 12V OK            : Yes

                        : 56V OK            : Yes

Main Board Temperatures         :

                        : U45 - LM95233 Local Temp     18 C (near DDR3)

                        : Q8  - LM95233 Remote 1 Temp   16 C (near intake right side edge)

                        : Q12 - LM95233 Remote 2 Temp   17 C (near SFP ports)

                        : U14 - ADT7476 Local Temp     24 C (near exhaust left side edge)
```

```
                    : U26 - ADT7476 Remote2 Temp    48 C (98DX3036 internal die temp)

Fan  0                      : 3474 rpm

Fan  1                      : 3375 rpm

Fan  2                      : 3463 rpm

Main Board Voltages         :

ispPAC_POWR1220AT8          :

                    : VDD_0V9           0.90V sense 0.928 V

                    : VDD_0V85          0.85V sense 0.870 V

                    : VDD_1V8           1.80V sense 1.844 V

                    : VDD_1V5           1.50V sense 1.554 V

                    : VDD_3V3           3.30V sense 3.396 V

                    : VDD_SW_1V8        1.80V sense 1.856 V

                    : VDD_SW_1V0        1.00V sense 1.022 V

                    : VDD_PHY_0V9       0.90V sense 0.928 V

                    : 3V3_SB            3.30V sense 3.378 V

                    : VDD_CPU           0.88V sense 0.894 V

                    : DDR3_VTT          0.77V sense 0.766 V
                    : VCC5              5.00V sense 5.022 V
```

注意　由于 VPNC 一定是使用硬件型号的控制器，所以针对该类型的 MD 控制器，这里的 Management MAC Address 地址和 HW MAC Addr 地址是一致的

Step3----在 VMM 上将 VPNC 停靠到指定的节点路径下

首先是添加 VPNC-1 的白名单，这里采用的是基于 MAC 地址的方式，而不是基于 IP 方式

```
(demo-mm) [mm] (config) #cd /mm

(demo-mm) [mm] (config) #local-peer-mac  00:0B:86:9A:D5:D7  ipsec  aruba123

(demo-mm) ^[mm] (config) #write me

Saving Configuration...

Configuration Saved.
```

注意　如果你的环境中有第二台 VPNC 时，请用上述的 CLI 再添加 VPNC-2 的白名单
例如 local-peer-mac 00:0B:86:9A:D5:D8 ipsec aruba123　，该 MAC 地址仅仅是演示使用，请用自己环境中的 VPNC 真实 MAC 地址来替换掉

接着查看下 **VPNC** 是否已经和 **VMM** 之间建立了 **ISAKMP SA**？

```
(demo-mm) [mm] (config) #show crypto isakmp sa

ISAKMP SA Active Session Information

------------------------------------

Initiator IP              Responder IP              Flags   Start Time      Private IP                Peer ID

------------               ------------             -----   ----------      ----------                -------------

172.16.220.200                10.1.101.10               r-v2-p   Feb  4 16:16:24   -                       00:0b:86:9a:d5:d7



Flags: i = Initiator; r = Responder  m = Main Mode; a = Agressive Mode; v2 = IKEv2

    p = Pre-shared key; c = Certificate/RSA Signature; e =  ECDSA Signature

    x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled

    3 = 3rd party AP; C = Campus AP; R = RAP;  Ru = Custom Certificate RAP; I = IAP

    V = VIA; S = VIA over TCP; l = uplink load-balance

Total ISAKMP SAs: 1
```

查看下 **VPNC** 是否已经和 **VMM** 之间建立了 **IPSec SA**？

```
(demo-mm) [mm] (config) #show crypto ipsec sa

IPSEC SA (V2) Active Session Information

-----------------------------------

Initiator IP                  Responder IP                  SPI(IN/OUT)     Flags Start Time     Inner IP                      Ipsec-map

------------                  ------------                  ----------------  ----- ---------------  --------                      ---------

172.16.220.200                   10.1.101.10                   253fef00/746b2600  UT2   Feb  4 16:16:24     -                       default-local-ma
ster-ipsecmap-00:0b:86:9a:d5:d7



Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap

    L = L2TP Tunnel; N = Nortel Client; C = Client; 2 = IKEv2

    I = uplink load-balance



Total IPSEC SAs: 1
```

最后我们来将 VPNC 停靠到指定的节点路径 下 /md/vpnc

```
注意，这里我们已经提前在 VMM 的 /md 下创建好了两个 节点路径，分别为：
```

```
/md/branch              Group      （用于停靠 Branch-MD 设备）

/md/vpnc                Group      （用于停靠 VPNC 设备）


(demo-mm) [mm] (config) #show switches

All Switches

------------

IP Address      IPv6 Address  Name      Location        Type    Model       Version       Status  Configuration State     Config Sync Time (sec)  Config ID

----------      ------------  ----      --------        ----    -----       -------       ------  -------------------     ----------------------  ---------

10.1.101.10     None          demo-mm   Building1.floor1  master  ArubaMM-VA  8.7.1.1_78245  up     UPDATE SUCCESSFUL       0                       2

172.16.220.200  None          demo-vpnc  Building1.floor1  MD     Aruba7010   8.7.1.1_78245  up     UNK(00:0b:86:9a:d5:d7)  N/A                     N/A


Total Switches:2

(demo-mm) [mm] (config) #configuration device 00:0b:86:9a:d5:d7 device-model A7010  /md/vpnc

(demo-mm) [mm] (config) #show configuration node-hierarchy


Default-node is not configured. Autopark is disabled.

Configuration node hierarchy
```

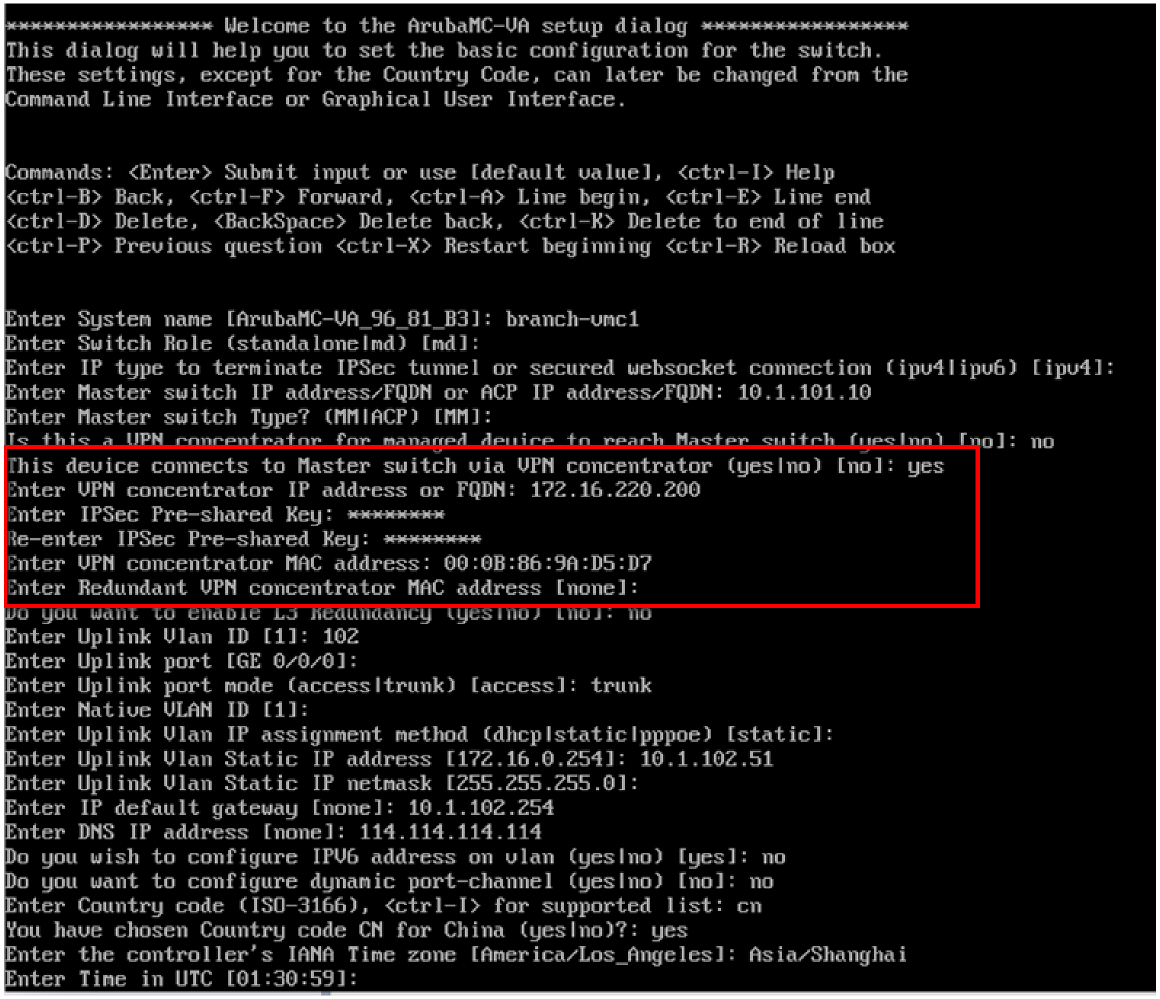
```
----------------------------

Config Node              Type    Name

-----------              ----    ----

/                       System

/md                     System

/md/branch              Group

/md/vpnc                Group

/md/vpnc/00:0b:86:9a:d5:d7   Device    demo-vpnc

/mm                     System

/mm/mynode              System
```

Step4----Branch-MD 的初始化，和常规的 MD 初始化不同，需要设置通过 VPNC 来连接 VMM。

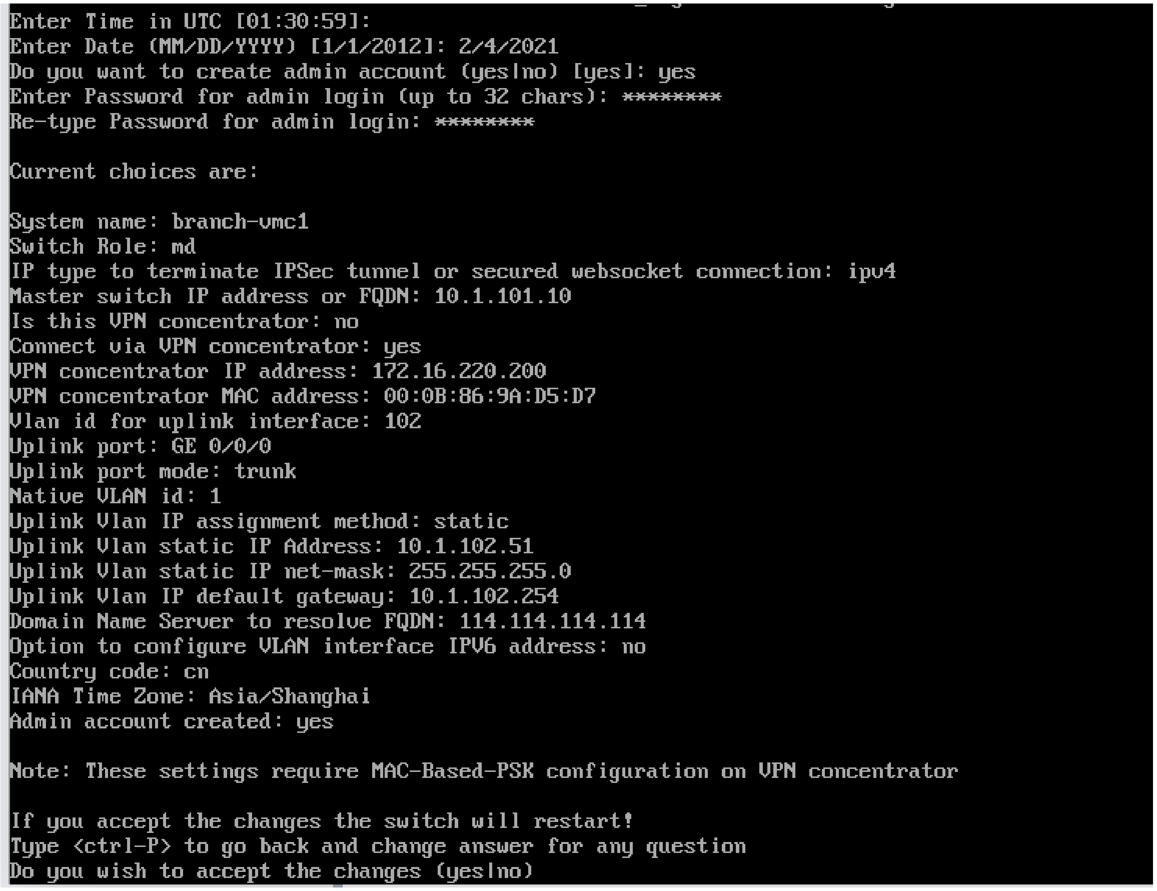
注意	本环境中 Branch-MD 采用 GE 0/0/0 口上联，并采用 Trunk 模式，Controller VLAN ID=102(初始化的时候也叫作 Uplink VLAN ID)，Native VLAN ID =1

首先进我们仍然选择 full-setup 模式，进入到配置向导。

```
Auto-provisioning is in progress. It requires DHCP and Activate servers

Choose one of the following options to override or debug auto-provisioning...

    'enable-debug'      : Enable auto-provisioning debug logs

    'disable-debug'     : Disable auto-provisioning debug logs

    'mini-setup'        : Start mini setup dialog. Provides minimal customization and requires DHCP server

    'full-setup'        : Start full setup dialog. Provides full customization

    'static-activate'   : Provides customization for static or PPPOE ip assignment. Uses activate for master information

Enter Option (partial string is acceptable): full-setup

Are you sure that you want to stop auto-provisioning and start full setup dialog? (yes/no): yes
```



```
***************** Welcome to the ArubaMC-VA setup dialog *****************
This dialog will help you to set the basic configuration for the switch.
These settings, except for the Country Code, can later be changed from the
Command Line Interface or Graphical User Interface.


Commands: <Enter> Submit input or use [default value], <ctrl-I> Help
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box


Enter System name [ArubaMC-VA_96_81_B3]: branch-vmc1
Enter Switch Role (standalone|md) [md]:
Enter IP type to terminate IPSec tunnel or secured websocket connection (ipv4|ipv6) [ipv4]:
Enter Master switch IP address/FQDN or ACP IP address/FQDN: 10.1.101.10
Enter Master switch Type? (MM|ACP) [MM]:
Is this a VPN concentrator for managed device to reach Master switch (yes|no) [no]: no
This device connects to Master switch via VPN concentrator (yes|no) [no]: yes
Enter VPN concentrator IP address or FQDN: 172.16.220.200
Enter IPSec Pre-shared Key: ********
Re-enter IPSec Pre-shared Key: ********
Enter VPN concentrator MAC address: 00:0B:86:9A:D5:D7
Enter Redundant VPN concentrator MAC address [none]:
Do you want to enable L3 Redundancy (yes|no) [no]: no
Enter Uplink Vlan ID [1]: 102
Enter Uplink port [GE 0/0/0]:
Enter Uplink port mode (access|trunk) [access]: trunk
Enter Native VLAN ID [1]:
Enter Uplink Vlan IP assignment method (dhcp|static|pppoe) [static]:
Enter Uplink Vlan Static IP address [172.16.0.254]: 10.1.102.51
Enter Uplink Vlan Static IP netmask [255.255.255.0]:
Enter IP default gateway [none]: 10.1.102.254
Enter DNS IP address [none]: 114.114.114.114
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
Do you want to configure dynamic port-channel (yes|no) [no]: no
Enter Country code (ISO-3166), <ctrl-I> for supported list: cn
You have chosen Country code CN for China (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]: Asia/Shanghai
Enter Time in UTC [01:30:59]:
```



```
Enter Time in UTC [01:30:59]:
Enter Date (MM/DD/YYYY) [1/1/2012]: 2/4/2021
Do you want to create admin account (yes|no) [yes]: yes
Enter Password for admin login (up to 32 chars): *********
Re-type Password for admin login: *********

Current choices are:

System name: branch-vmc1
Switch Role: md
IP type to terminate IPSec tunnel or secured websocket connection: ipv4
Master switch IP address or FQDN: 10.1.101.10
Is this VPN concentrator: no
Connect via VPN concentrator: yes
VPN concentrator IP address: 172.16.220.200
VPN concentrator MAC address: 00:0B:86:9A:D5:D7
Vlan id for uplink interface: 102
Uplink port: GE 0/0/0
Uplink port mode: trunk
Native VLAN id: 1
Uplink Vlan IP assignment method: static
Uplink Vlan static IP Address: 10.1.102.51
Uplink Vlan static IP net-mask: 255.255.255.0
Uplink Vlan IP default gateway: 10.1.102.254
Domain Name Server to resolve FQDN: 114.114.114.114
Option to configure VLAN interface IPV6 address: no
Country code: cn
IANA Time Zone: Asia/Shanghai
Admin account created: yes

Note: These settings require MAC-Based-PSK configuration on VPN concentrator

If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no)
```

最后输入 yes，重启 Branch MD.

注意	在初始化向导中，如果你的环境中存在两台 VPNC，那还需要设置 Redundancy VPN concentrator MAC address 指向到 VPNC-2.

等 Branch-MD 重启完成后，接着查看并记录 Management MAC Address，为了允许 Branch-MD 和 VPNC 之间的通讯，这个 Branch-MD 的 Management MAC Address 地址是需要的，会在后续的 VPNC 上的 vpn-peer peer-mac 命令中使用到。

```
(branch-vmc1) #show interface mgmt

mgmt is administratively down line protocol is down

Hardware is Ethernet, address is 00:0C:29:96:81:A9



(branch-vmc1) #show inventory

Mgmt Port HW MAC Addr          : 00:0C:29:96:81:A9            （由于本环境采用的是 VMC，这个地址是 Branch-MD 的 Management MAC Address）

HW MAC Addr                     : 00:0C:29:96:81:B3            （用于 VMC 停靠节点路径）

Product key#                 : MC39681A9

Activate license             : Not Applicable

Active device type             : MC-VA-10
```

注意

针对 VMC，这里的 Mgmt Port HW MAC Addr 地址和 HW MAC Addr 地址**是不一致的**，我们需要的是 Mgmt Port HW MAC Addr（也就是 Branch-MD 的 Management MAC Address）

如果你的环境中使用的是硬件类型的 Branch-MD 控制器，请参考本手册 VPNC 中的获取 Management MAC Address 的方式，方法是一样的。

Step5----在 VMM 上的 VPNC 设备节点下，配置 Branch-MD 的白名单

```
(demo-mm) [mynode] #show configuration node-hierarchy

Default-node is not configured. Autopark is disabled.

Configuration node hierarchy

----------------------------

Config Node              Type    Name

-----------              ----    ----

/                        System

/md                      System

/md/branch               Group

/md/vpnc                 Group

/md/vpnc/00:0b:86:9a:d5:d7  Device  demo-vpnc

/mm                      System

/mm/mynode               System

(demo-mm) [mynode] #cd   demo-vpnc         （在 VMM 上，进入到 VPNC 的设备节点下）
```

```
(demo-mm) [00:0b:86:9a:d5:d7] #configure terminal

Enter Configuration commands, one per line. End with CNTL/Z

(demo-mm) [00:0b:86:9a:d5:d7] (config) #vpn-peer peer-mac 00:0C:29:96:81:A9 pre-share-key aruba123    （在 VPNC 上配置 Branch-MD 的白名单）

(demo-mm) ^[00:0b:86:9a:d5:d7] (config) #end

 (demo-mm) ^[00:0b:86:9a:d5:d7] #write me

Saving Configuration...

Configuration Saved.



(demo-mm) [mm] #show switches

All Switches

------------

IP Address     IPv6 Address  Name        Location         Type    Model       Version       Status  Configuration State     Config Sync Time (sec)  Config ID

----------     ------------  ----        --------         ----    -----       -------       ------  -------------------     ---------------------   ---------

10.1.101.10     None        demo-mm      Building1.floor1  master  ArubaMM-VA  8.7.1.1_78245  up     UPDATE SUCCESSFUL      0                  3

172.16.220.200  None        demo-vpnc    Building1.floor1  MD      Aruba7010   8.7.1.1_78245  up     UPDATE SUCCESSFUL      8                  3

10.1.102.51     None        branch-vmc1  Building1.floor1  MD      ArubaMC-VA  8.7.1.1_78245  up     UNK(00:0c:29:96:81:b3)  N/A               N/A

Total Switches:3
```

此时，已经可以在 VMM 上看到了新上线的 Branch-MD 了

注意

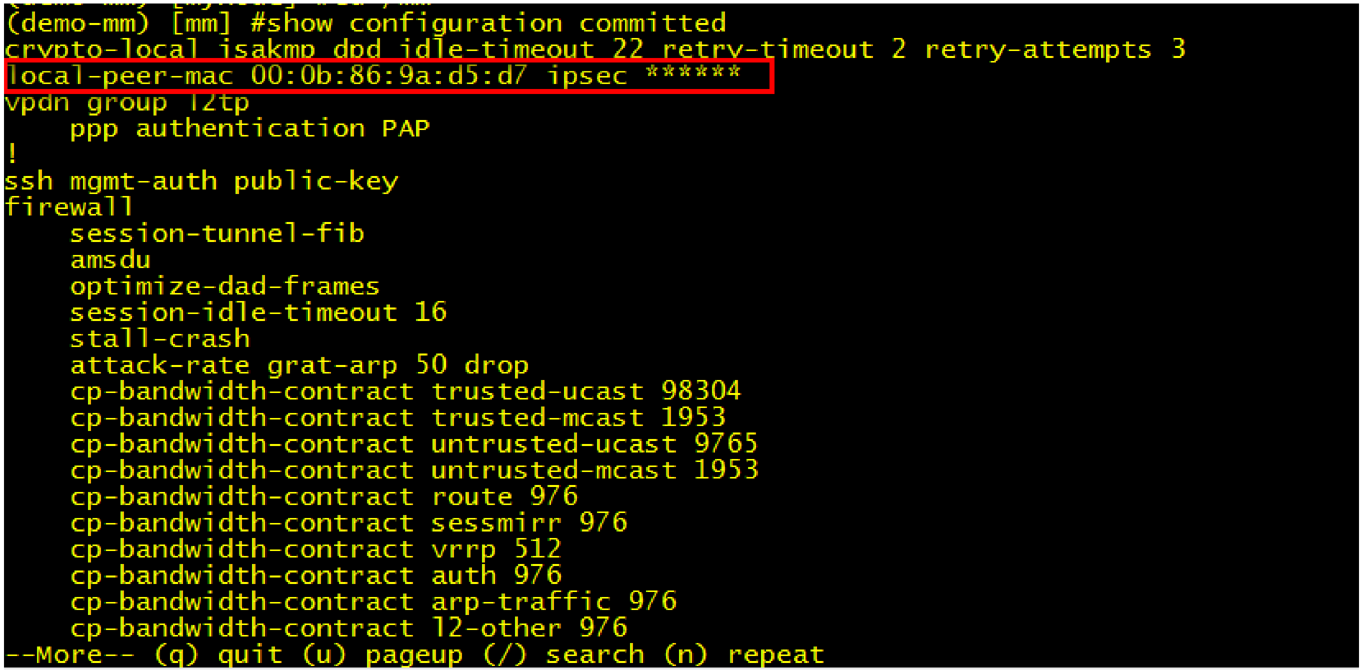
有多台的 Branch-MD 控制器，请在该 VPNC 上增加配置多个 Branch-MD 的白名单，例如：

```
vpn-peer peer-mac 00:0C:29:96:81:A6  pre-share-key aruba123
vpn-peer peer-mac 00:0C:29:96:81:A7  pre-share-key aruba123
```

Step6----在 VMM 上停靠 Branch-MD 到指定的节点路径下

由于 **VMM** 上只要添加 **VPNC** 的白名单，无需添加 **Branch-MD** 的白名单（仅需要在 **VPNC** 上添加 **Branch-MD** 的白名单）。因为 **VMM** 只要和 **VPNC** 建立一个 **IPSec** 隧道，通过该隧道可以同时接管 **VPNC** 和 **Branch-MD**。

下图是在 **VMM** 上看到的仅添加 **VPNC** 的白名单设置。



```
(demo-mm) [mm] #show configuration committed
crypto-local isakmp dpd idle-timeout 22 retry-timeout 2 retry-attempts 3
local-peer-mac 00:0b:86:9a:d5:d7 ipsec ******
vpdn group l2tp
    ppp authentication PAP
!
ssh mgmt-auth public-key
firewall
    session-tunnel-fib
    amsdu
    optimize-dad-frames
    session-idle-timeout 16
    stall-crash
    attack-rate grat-arp 50 drop
    cp-bandwidth-contract trusted-ucast 98304
    cp-bandwidth-contract trusted-mcast 1953
    cp-bandwidth-contract untrusted-ucast 9765
    cp-bandwidth-contract untrusted-mcast 1953
    cp-bandwidth-contract route 976
    cp-bandwidth-contract sessmirr 976
    cp-bandwidth-contract vrrp 512
    cp-bandwidth-contract auth 976
    cp-bandwidth-contract arp-traffic 976
    cp-bandwidth-contract l2-other 976
--More-- (q) quit (u) pageup (/) search (n) repeat
```

将刚刚上线的 **Branch-MD** 手动停靠到指定的 **/md/branch** 节点路径下。

注意

针对 VMC，将设备停靠到指定的节点路径下，这里需要的 MAC 地址是 HW MAC Addr 地址。

```
(branch-vmc1) #show inventory
Mgmt Port HW MAC Addr        : 00:0C:29:96:81:A9
HW MAC Addr                  : 00:0C:29:96:81:B3          （用于 VMC 停靠节点路径）
Product key#                 : MC39681A9
Activate license             : Not Applicable
Active device type           : MC-VA-10
```

```
(demo-mm) [mm] (config) #configuration device  00:0c:29:96:81:b3  device-model  mc-va    /md/branch

(demo-mm) [mm] (config) #show configuration node-hierarchy

Default-node is not configured. Autopark is disabled.

Configuration node hierarchy

----------------------------

Config Node                  Type    Name

-----------                  ----    ----

/                            System

/md                          System

/md/branch                   Group

/md/branch/00:0c:29:96:81:b3  Device  branch-vmc1

/md/vpnc                     Group

/md/vpnc/00:0b:86:9a:d5:d7    Device  demo-vpnc

/mm                          System

/mm/mynode                   System
```

```
(demo-mm) [mm] (config) #show switches


All Switches

------------

IP Address     IPv6 Address  Name        Location        Type    Model      Version      Status  Configuration State  Config Sync Time (sec)  Config ID

----------     ------------  ----        --------        ----    -----      -------      ------  -------------------  ----------------------  ---------

10.1.101.10    None          demo-mm     Building1.floor1  master  ArubaMM-VA  8.7.1.1_78245  up    UPDATE SUCCESSFUL    0                       3

172.16.220.200  None         demo-vpnc   Building1.floor1  MD     Aruba7010   8.7.1.1_78245   up    UPDATE SUCCESSFUL    8                       3

10.1.102.51    None          branch-vmc1  Building1.floor1  MD     ArubaMC-VA  8.7.1.1_78245  up    UPDATE SUCCESSFUL    10                      3


Total Switches:3
```

至此，我们的 VMM，VPNC 和 Branch-MD 都已经上线了，大家有可以自己尝试去实现主备 VMM，主备 VPNC 的相关设置。

对于其他分支控制器的配置，请重复 Branch-MD 的上线步骤即可，同时也需要在 VPNC 上增加相应的 Branch-MD 的白名单。

Step7----查看一些连接状态

查看 VMM 上有一个到 Branch-MD 的路由记录，下一跳是指向 VPNC 的 IPSec 隧道。

同时也有一个到 VPNC 的路由记录，下一跳也是指向 VPNC 的 IPSec 隧道。

```
 (demo-mm) [mm] (config) #show ip route

Codes: C - connected, O - OSPF, R - RIP, S - static, B - Bgw peer uplink

       M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN/Branch

       I - Ike-overlay, N - not redistributed

Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10

Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10

Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10

Gateway of last resort is 10.1.101.254 to network 0.0.0.0 at cost 1

S*    0.0.0.0/0  [0/1] via 10.1.101.254*

S    10.1.102.51/32   [0/20]    ipsec map     default-local-master-ipsecmap-00:0b:86:9a:d5:d7

C    10.1.101.0/24 is directly connected, VLAN101

C    172.16.220.200/32   is an ipsec map   default-local-master-ipsecmap-00:0b:86:9a:d5:d7
```

查看 **Branch-MD** 上有一个到 **VMM** 的路由记录，下一跳指向 **VPNC** 的 **IPSec** 隧道。

同时也有一个到 **VPNC** 的路由记录，下一跳也是指向 **VPNC** 的 **IPSec** 隧道。

```
(branch-vmc1) #show ip route

Codes: C - connected, O - OSPF, R - RIP, S - static, B - Bgw peer uplink

       M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN/Branch

       I - Ike-overlay, N - not redistributed

Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10

Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10

Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10

Gateway of last resort is 10.1.102.254 to network 0.0.0.0 at cost 1

S*    0.0.0.0/0  [0/1] via 10.1.102.254*

I    10.1.101.10/32 [0/256] ipsec map  management-vpnc

C    10.1.102.0/24 is directly connected, VLAN102

C    172.16.220.200/32 is an ipsec map  management-vpnc
```

在 **Branch-MD** 上分别去 **ping VMM** 和 **VPNC**，都能够正常通讯。

```
(branch-vmc1) #ping 10.1.101.10
Press 'q' to abort.
Sending 5, 92-byte ICMP Echos to 10.1.101.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3.677/4.1286/4.786 ms


(branch-vmc1) #ping 172.16.220.200
Press 'q' to abort.
Sending 5, 92-byte ICMP Echos to 172.16.220.200, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2.062/2.4982/2.743 ms
```

在 **Branch-MD** 上查看 **ISAKMP** 和 **IPSec SA**，状态都正常，和 **VPNC** 建立 **IPSec** 隧道。

```
(branch-vmc1) #show crypto isakmp sa
```

```
ISAKMP SA Active Session Information

-----------------------------------

Initiator IP             Responder IP            Flags   Start Time     Private IP                 Peer ID

------------              ------------            -----  ----------    ----------                 -------------

10.1.102.51               172.16.220.200          i-v2-p  Feb  4 10:20:07   -                      00:0b:86:9a:d5:d7


Flags: i = Initiator; r = Responder

    m = Main Mode; a = Agressive Mode; v2 = IKEv2

    p = Pre-shared key; c = Certificate/RSA Signature; e =  ECDSA Signature

    x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled

    3 = 3rd party AP; C = Campus AP; R = RAP;  Ru = Custom Certificate RAP; I = IAP

    V = VIA; S = VIA over TCP; l = uplink load-balance


Total ISAKMP SAs: 1


(branch-vmc1) #show crypto ipsec sa
```

```
IPSEC SA (V2) Active Session Information

-----------------------------------

Initiator IP              Responder IP              SPI(IN/OUT)      Flags Start Time      Inner IP                Ipsec-map

------------              ------------              ----------------   ----- ---------------   --------                ---------

10.1.102.51               172.16.220.200            f1885600/6fd3ff00  UT2   Feb  4 10:20:06     -                     management-vpnc


Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap

    L = L2TP Tunnel; N = Nortel Client; C = Client; 2 = IKEv2

    l = uplink load-balance


Total IPSEC SAs: 1


(branch-vmc1) #show crypto map

Crypto Map "management-vpnc" 9999 ipsec-isakmp

Crypto Map Template"management-vpnc" 9999

     IKE Version: 2

     IKEv2 Policy: 10014
```

```
Security association lifetime seconds : [300 -86400]
Security association lifetime kilobytes: N/A
PFS (Y/N): N
Transform sets={ default-3rd-ikev2-transform }
Peer gateway: 172.16.220.200
Monitor IP: 0.0.0.0
Peer MAC: "00:0B:86:9A:D5:D7"
Interface: VLAN 102
Source network: 10.1.102.51/255.255.255.255
Destination network: 172.16.220.200/255.255.255.255
Pre-Connect (Y/N): Y
Client NAT mode (Y/N): N
Tunnel Trusted (Y/N): Y
Forced NAT-T (Y/N): Y
Uplink Failover (Y/N): N
Force-Tunnel-Mode (Y/N): N
Uplink LoadBalance (Y/N): N
```

```
        IP Compression (Y/N): Y
        DPD counters req_initd:1 req_resent:0 reply_recvd:1 peer_dead:0
        DPD counters req_recvd:0 reply_sent:0
        XCHG counters peer dead:0
        CFG_SET Initiate Sent/Retry-NoACK/Retry-NoVLAN/Ack-Recvd= 0/0/0/0
        CFG_SET Responder Recvd/Ack-sent= 0/0
        Tunnel status IPSEC: UP IKE: UP
Crypto Map "GLOBAL-IKEV2-MAP" 10000 ipsec-isakmp
Crypto Map Template"default-rap-ipsecmap" 10001
        IKE Version: 2
        IKEv2 Policy: DEFAULT
        Security association lifetime seconds : [300 -86400]
        Security association lifetime kilobytes: N/A
        PFS (Y/N): N
        Transform sets={ default-gcm256, default-gcm128, default-rap-transform }
Crypto Map "GLOBAL-MAP" 10000 ipsec-isakmp
Crypto Map Template"default-dynamicmap" 10000
```

```
        IKE Version: 1

        IKEv1 Policy: All

        Security association lifetime seconds : [300 -86400]

        Security association lifetime kilobytes: N/A

        PFS (Y/N): N

        Transform sets={ default-transform, default-aes }

```

在 Branch-MD 上 show switches，状态显示更新成功。

```
(branch-vmc1) #show switches



All Switches

------------

IP Address   IPv6 Address  Name        Location        Type  Model       Version       Status  Configuration State  Config Sync Time (sec)  Config ID
```

```
----------   ------------  ----       --------       ----  -----     -------      ------  -------------------  ----------------------  ---------

10.1.102.51  None       branch-vmc1  Building1.floor1  MD   ArubaMC-VA  8.7.1.1_78245  up    UPDATE SUCCESSFUL   10               3



Total Switches:1
```

查看 VPNC 上有一个到 VMM 的路由记录，下一跳指向 VMM 的 IPSec 隧道。

同时也有一个到 Branch-MD 的路由记录，下一跳是指向 Branch-MD 的 IPSec 隧道。

```
(demo-vpnc) [MDC] #show ip route

Codes: C - connected, O - OSPF, R - RIP, S - static, B - Bgw peer uplink

       M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN/Branch

       I - Ike-overlay, N - not redistributed

Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10

Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10

Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10

Gateway of last resort is 172.16.220.254 to network 0.0.0.0 at cost 1
```

```
S*    0.0.0.0/0  [0/1] via 172.16.220.254*

C    172.16.220.128/25 is directly connected, VLAN23

C    10.1.101.10/32 is an ipsec map    default-local-master-ipsecmap                          （到 VMM 的主机路由）

C    10.1.102.51/32 is an ipsec map    default-vpnip-master-ipsecmap-00:0c:29:96:81:a9        （到 Branch-MD 的主机路由）
```

在 VPNC 上查看 ISAKMP 和 IPSec SA，状态都正常，分别和 VMM 和 Branch-MD 建立了 IPSec 隧道。

```
(demo-vpnc) [MDC] # show crypto map


Crypto Map "default-vpnip-master-ipsecmap-00:0c:29:96:81:a9" 9999 ipsec-isakmp      （到 Branch-MD 的 IPSec 隧道）

Crypto Map Template"default-vpnip-master-ipsecmap-00:0c:29:96:81:a9" 9999

        IKE Version: 2

        IKEv2 Policy: 10014

        Security association lifetime seconds : [300 -86400]

        Security association lifetime kilobytes: N/A
```

```
PFS (Y/N): N
Transform sets={ default-3rd-ikev2-transform }
Peer gateway: 0.0.0.0/::
Monitor IP: 0.0.0.0
Peer MAC: "00:0c:29:96:81:a9"
Interface: VLAN 0
Source network: 172.16.220.200/255.255.255.255
Destination network: 10.1.102.51/255.255.255.255
Pre-Connect (Y/N): N
Client NAT mode (Y/N): N
Tunnel Trusted (Y/N): Y
Forced NAT-T (Y/N): Y
Uplink Failover (Y/N): N
Force-Tunnel-Mode (Y/N): N
Uplink LoadBalance (Y/N): N
IP Compression (Y/N): Y
DPD counters req_initd:0 req_resent:0 reply_recvd:0 peer_dead:0
```

```
        DPD counters req_recvd:1 reply_sent:1

        XCHG counters peer dead:0

        CFG_SET Initiate Sent/Retry-NoACK/Retry-NoVLAN/Ack-Recvd= 0/0/0/0

        CFG_SET Responder Recvd/Ack-sent= 0/0

        Tunnel status IPSEC: UP IKE: UP

Crypto Map "default-local-master-ipsecmap" 9999 ipsec-isakmp          （到 VMM 的 IPSec 隧道）

Crypto Map Template"default-local-master-ipsecmap" 9999

        IKE Version: 2

        IKEv2 Policy: 10014

        Security association lifetime seconds : [300 -86400]

        Security association lifetime kilobytes: N/A

        PFS (Y/N): N

        Transform sets={ default-3rd-ikev2-transform }

        Peer gateway: 10.1.101.10

        Monitor IP: 0.0.0.0

        Peer MAC: "00:0C:29:37:E5:44"

        Interface: VLAN 23
```

```
      Source network: 172.16.220.200/255.255.255.255

      Destination network: 10.1.101.10/255.255.255.255

      Pre-Connect (Y/N): Y

      Client NAT mode (Y/N): N

      Tunnel Trusted (Y/N): Y

      Forced NAT-T (Y/N): Y

      Uplink Failover (Y/N): N

      Force-Tunnel-Mode (Y/N): N

      Uplink LoadBalance (Y/N): N

      IP Compression (Y/N): N

      DPD counters req_initd:1 req_resent:0 reply_recvd:1 peer_dead:0

      DPD counters req_recvd:0 reply_sent:0

      XCHG counters peer dead:0

      CFG_SET Initiate Sent/Retry-NoACK/Retry-NoVLAN/Ack-Recvd= 0/0/0/0

      CFG_SET Responder Recvd/Ack-sent= 0/0

      Tunnel status IPSEC: UP IKE: UP

Crypto Map "GLOBAL-IKEV2-MAP" 10000 ipsec-isakmp
Crypto Map Template"default-rap-ipsecmap" 10001
      IKE Version: 2
      IKEv2 Policy: DEFAULT
      Security association lifetime seconds : [300 -86400]
      Security association lifetime kilobytes: N/A
      PFS (Y/N): N
      Transform sets={ default-gcm256, default-gcm128, default-rap-transform }
Crypto Map "GLOBAL-MAP" 10000 ipsec-isakmp
Crypto Map Template"default-dynamicmap" 10000
      IKE Version: 1
      IKEv1 Policy: All
      Security association lifetime seconds : [300 -86400]
      Security association lifetime kilobytes: N/A
      PFS (Y/N): N
      Transform sets={ default-transform, default-aes }

(demo-vpnc) [MDC] #show crypto isakmp sa
```

```
ISAKMP SA Active Session Information

------------------------------------

Initiator IP              Responder IP              Flags    Start Time       Private IP                Peer ID

------------              ------------              -----   ----------       ----------                -------------

172.16.220.200               10.1.101.10              i-v2-p    Feb  4 16:01:17     -                       00:0c:29:37:e5:44

10.1.102.51                 172.16.220.200            r-v2-p    Feb  4 17:24:18     -                       00:0c:29:96:81:a9


Flags: i = Initiator; r = Responder

    m = Main Mode; a = Agressive Mode; v2 = IKEv2

    p = Pre-shared key; c = Certificate/RSA Signature; e =  ECDSA Signature

    x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled

    3 = 3rd party AP; C = Campus AP; R = RAP;  Ru = Custom Certificate RAP; I = IAP

    V = VIA; S = VIA over TCP; l = uplink load-balance


Total ISAKMP SAs: 2
```

```
(demo-vpnc) [MDC] #show crypto ipsec sa

IPSEC SA (V2) Active Session Information

-----------------------------------

Initiator IP              Responder IP             SPI(IN/OUT)      Flags Start Time       Inner IP                  Ipsec-map

------------              ------------             ----------------  ----- ---------------  --------                  ---------

10.1.102.51               172.16.220.200            6fd3ff00/f1885600  UT2   Feb  4 17:24:17     -                     default-vpnip-ma
ster-ipsecmap-00:0c:29:96:81:a9

172.16.220.200            10.1.101.10               27c54700/eaef9300  UT2   Feb  4 17:56:18     -                     default-local-ma
ster-ipsecmap


Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap

    L = L2TP Tunnel; N = Nortel Client; C = Client; 2 = IKEv2

    l = uplink load-balance


Total IPSEC SAs: 2
```

**2）	VPNC 和 Branch-MD 已经采用常规的 MD 上线方式配置好，且都已经成功停靠到 VMM 的指定节点路径 /md/campus 下，在这个情况下，VMM 上该如何调整配置？如何将总部的一台 MD 转换成 VPNC 角色？针对已经在 VMM 上停靠好的 Branch-MD，如何重新指向到 VPNC 呢？**

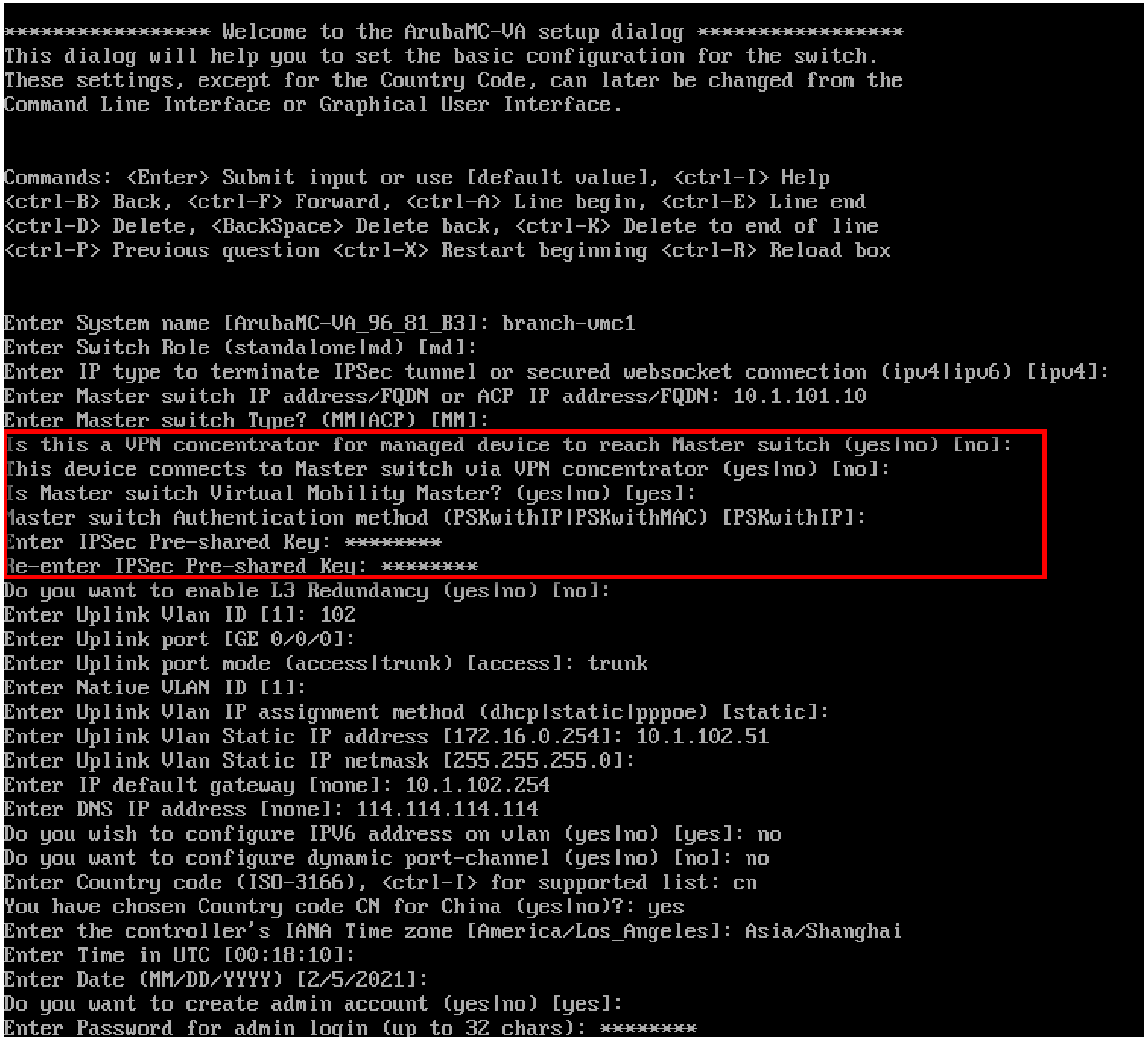
大多数同学首先想到的是需要对已有的 **VMM**，**VPNC** 和 **Branch-MD** 重新都走一遍初始化向导不就可以完成设置吗，对的，确实如果所有的设备按照之前介绍的初始化向导（采用 **pskwithmac** 认证方式）走一遍，会非常方便地完成 **VMM**，**VPNC** 和 **Branch-MD** 的配置，但本阶段的配置前提是所有的 **VMM**，**VPNC** 和 **Branch-MD** 都完成了常规的初始化向导配置，且都是按照 **pskwithip** 认证的普通 **MD** 方式上线了（即所有的 **MD** 都直接指向 **VMM**，和 **VMM** 之间直接建立了 **IPSec** 隧道，并没有指定其中一台 **MD** 为 **VPNC** 角色），问题就在于一开始初始化向导时，并没有按照 **VPNC** 的方式来配置，且所有 **MD** 已经完成了初始化向导，系统也正常工作了，同时客户的无线网络也已经正常使用了，不允许你过多的断网，重新调试且需要重启过多设备的前提下，该如何解决呢？

1）是否有相关的配置，即可以保证 **VMM** 和 **VPNC**（即从最初的 **MD** 转成 **VPNC** 角色）的配置变更，又不需要重启或者再次初始化 **VMM** 和 **VPNC** 呢？

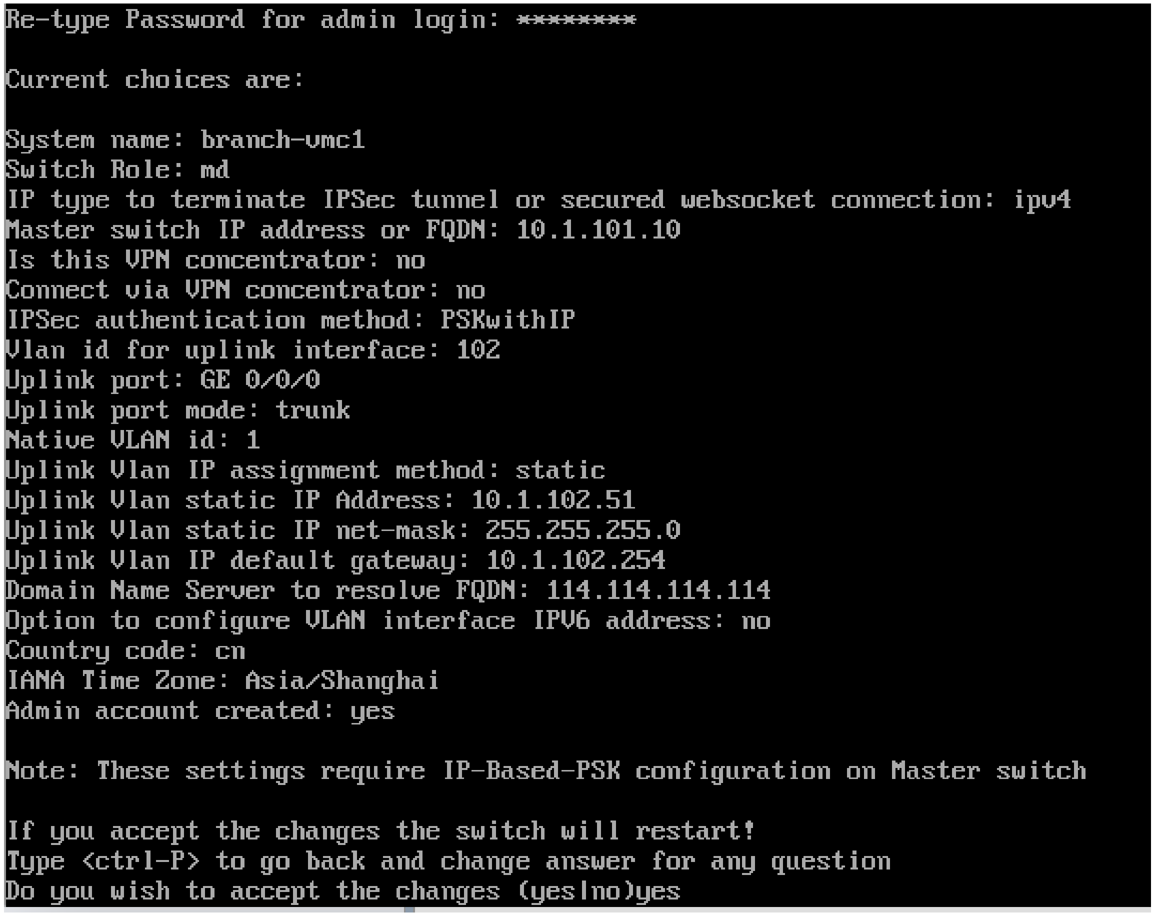
2）对于分支 **Branch-MD** 的配置变更，由于本身属于新增上线设备的调试阶段，是否可以允许重启一次或者走一遍初始化呢？

在常规配置模式下，你会在 **VMM** 上看到 **2** 台 **MD** 上线，并且 **VMM** 会分别建立隧道到两台 **MD**，即存在两条 **IPSec** 隧道，也就是说每台 **MD** 是直接指向到 **VMM** 上线的，并且 **VMM** 上直接通过 **localip** 来添加了两台 **MD** 的白名单。

常规模式下所有 **MD** 初始化上线的操作如下，你会发现并没有设置 **VPNC** 的相关内容。



```
***************** Welcome to the ArubaMC-VA setup dialog *****************
This dialog will help you to set the basic configuration for the switch.
These settings, except for the Country Code, can later be changed from the
Command Line Interface or Graphical User Interface.


Commands: <Enter> Submit input or use [default value], <ctrl-I> Help
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box


Enter System name [ArubaMC-VA_96_81_B3]: branch-vmc1
Enter Switch Role (standalone|md) [md]:
Enter IP type to terminate IPSec tunnel or secured websocket connection (ipv4|ipv6) [ipv4]:
Enter Master switch IP address/FQDN or ACP IP address/FQDN: 10.1.101.10
Enter Master switch Type? (MM|ACP) [MM]:
Is this a VPN concentrator for managed device to reach Master switch (yes|no) [no]:
This device connects to Master switch via VPN concentrator (yes|no) [no]:
Is Master switch Virtual Mobility Master? (yes|no) [yes]:
Master switch Authentication method (PSKwithIP|PSKwithMAC) [PSKwithIP]:
Enter IPSec Pre-shared Key: ********
Re-enter IPSec Pre-shared Key: ********
Do you want to enable L3 Redundancy (yes|no) [no]:
Enter Uplink Vlan ID [1]: 102
Enter Uplink port [GE 0/0/0]:
Enter Uplink port mode (access|trunk) [access]: trunk
Enter Native VLAN ID [1]:
Enter Uplink Vlan IP assignment method (dhcp|static|pppoe) [static]:
Enter Uplink Vlan Static IP address [172.16.0.254]: 10.1.102.51
Enter Uplink Vlan Static IP netmask [255.255.255.0]:
Enter IP default gateway [none]: 10.1.102.254
Enter DNS IP address [none]: 114.114.114.114
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
Do you want to configure dynamic port-channel (yes|no) [no]: no
Enter Country code (ISO-3166), <ctrl-I> for supported list: cn
You have chosen Country code CN for China (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]: Asia/Shanghai
Enter Time in UTC [00:18:10]:
Enter Date (MM/DD/YYYY) [2/5/2021]:
Do you want to create admin account (yes|no) [yes]:
Enter Password for admin login (up to 32 chars): ********
```



```
Re-type Password for admin login: ********

Current choices are:

System name: branch-vmc1
Switch Role: md
IP type to terminate IPSec tunnel or secured websocket connection: ipv4
Master switch IP address or FQDN: 10.1.101.10
Is this VPN concentrator: no
Connect via VPN concentrator: no
IPSec authentication method: PSKwithIP
Vlan id for uplink interface: 102
Uplink port: GE 0/0/0
Uplink port mode: trunk
Native VLAN id: 1
Uplink Vlan IP assignment method: static
Uplink Vlan static IP Address: 10.1.102.51
Uplink Vlan static IP net-mask: 255.255.255.0
Uplink Vlan IP default gateway: 10.1.102.254
Domain Name Server to resolve FQDN: 114.114.114.114
Option to configure VLAN interface IPV6 address: no
Country code: cn
IANA Time Zone: Asia/Shanghai
Admin account created: yes

Note: These settings require IP-Based-PSK configuration on Master switch

If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no)yes
```

在 **VMM** 上，可以看到所有 **MD** 都已经停靠到指定的节点路径 **/md/campus**（举例）下，每台 **MD** 都分别建立了 **IPSec** 隧道到 **VMM**，那么 **2** 台 **MD** 就会在 **VMM** 上创建了 **2** 条 **IPSec** 隧道。

```
(demo-mm) [mm] (config) #show configuration node-hierarchy

Default-node is not configured. Autopark is disabled.

Configuration node hierarchy

----------------------------

Config Node                  Type    Name

-----------                  ----    ----

/                          System

/md                          System

/md/branch                   Group

/md/campus                   Group

/md/campus/00:0b:86:9a:d5:d7     Device   demo-vpnc

/md/campus/00:0c:29:96:81:b3     Device   branch-vmc1

/md/vpnc                     Group

/mm                          System

/mm/mynode                   System



(demo-mm) [mm] (config) #show configuration committed
```

```
crypto-local isakmp dpd idle-timeout 22 retry-timeout 2 retry-attempts 3

localip 172.16.220.200 ipsec ******

localip 10.1.102.51 ipsec ******

vpdn group l2tp

   ppp authentication PAP

!



(demo-mm) [mm] (config) #show switches

All Switches

------------

IP Address     IPv6 Address  Name        Location         Type    Model      Version      Status  Configuration State  Config Sync Time (sec)  Config ID

----------     ------------  ----        --------         ----    -----      -------      ------  -------------------  ----------------------  ---------

10.1.101.10     None         demo-mm     Building1.floor1  master  ArubaMM-VA  8.7.1.1_78245  up     UPDATE SUCCESSFUL    0                   4

172.16.220.200  None         demo-vpnc   Building1.floor1  MD      Aruba7010   8.7.1.1_78245  up     UPDATE SUCCESSFUL    10                  4

10.1.102.51     None         branch-vmc1 Building1.floor1  MD      ArubaMC-VA  8.7.1.1_78245  up     UPDATE SUCCESSFUL    10                  4


Total Switches:3
```

```
(demo-mm) [mm] (config) #show crypto isakmp sa

ISAKMP SA Active Session Information

-----------------------------------

Initiator IP                Responder IP                Flags    Start Time        Private IP                  Peer ID

------------                 ------------                 -----   ----------        ----------                  -------------

172.16.220.200                10.1.101.10                   r-v2-p   Feb  5 15:27:12    -                          IPV4_ADDR:172.16.220.200

10.1.102.51                   10.1.101.10                   r-v2-p   Feb  5 15:49:49    -                          IPV4_ADDR:10.1.102.51

Flags: i = Initiator; r = Responder

     m = Main Mode; a = Agressive Mode; v2 = IKEv2

     p = Pre-shared key; c = Certificate/RSA Signature; e =  ECDSA Signature

     x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled

     3 = 3rd party AP; C = Campus AP; R = RAP;  Ru = Custom Certificate RAP; I = IAP

     V = VIA; S = VIA over TCP; l = uplink load-balance

Total ISAKMP SAs: 2
```

```
(demo-mm) [mm] (config) #show crypto ipsec sa

IPSEC SA (V2) Active Session Information

-----------------------------------

Initiator IP                    Responder IP                     SPI(IN/OUT)       Flags Start Time       Inner IP                          Ipsec-map

------------                     ------------                    ----------------    ----- ---------------    --------                          ---------

10.1.102.51                       10.1.101.10                      9fd9a600/b1360500  UT2   Feb  5 15:49:50     -                                   default-local-mast
er-ipsecmap10.1.102.51

172.16.220.200                    10.1.101.10                      3a049f00/b550ef00  UT2   Feb  5 15:27:12     -                                   default-local-ma
ster-ipsecmap172.16.220.200


Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap

     L = L2TP Tunnel; N = Nortel Client; C = Client; 2 = IKEv2

     l = uplink load-balance


Total IPSEC SAs: 2
```

那接下来，针对已经上线的 MD，我们需要调整的配置如下：

Step1----在 VPNC(本环境中的 Hostname=demo-vpnc)控制器上进行配置调整

在 VMM 控制器上，进入到设备节点 /md/campus/00:0b:86:9a:d5:d7（我们会规划这台 MD 作为 VPNC 角色），也就是 demo-vpnc 下配置：

```
(demo-mm) [mm] #show configuration node-hierarchy

Default-node is not configured. Autopark is disabled.

Configuration node hierarchy

----------------------------

Config Node                  Type    Name

-----------                  ----    ----

/                       System

/md                       System

/md/campus                    Group

/md/campus/00:0b:86:9a:d5:d7  Device  demo-vpnc

/md/campus/00:0c:29:96:81:b3  Device   branch-vmc1

/mm                       System

/mm/mynode                    System
```

```
(demo-mm) [mm] #cd   demo-vpnc                              （进入到 hostname=demo-vpnc 的设备节点下）

(demo-mm) [00:0b:86:9a:d5:d7] #configure terminal

Enter Configuration commands, one per line. End with CNTL/Z

 (demo-mm) [00:0b:86:9a:d5:d7] (config) #vpn-peer peer-mac 00:0C:29:96:81:A9 pre-share-key aruba123  （在 VPNC 上配置 Branch-MD 的白名单）

(demo-mm) ^[00:0b:86:9a:d5:d7] (config) #write me

Saving Configuration...

Configuration Saved.
```

注意

如果存在多个 Branch-MD 的环境，我们重复输入上述的 CLI 即可，例如：

```
vpn-peer peer-mac 00:0C:29:96:81:A8  pre-share-key aruba123
vpn-peer peer-mac 00:0C:29:96:81:A7  pre-share-key aruba123
vpn-peer peer-mac 00:0C:29:96:81:A6  pre-share-key aruba123
```

Step2----在 Branch-MD（本环境中的 Hostname=branch-vmc1）控制器上进行配置调整

在 VMM 控制器上，进入到设备节点 /md/campus/00:0c:29:96:81:b3（我们会规划这台 MD 作为 Branch-MD 角色）， 也就是 branch-vmc1 下配置：

```
(demo-mm) [mynode] (config) #show configuration node-hierarchy

Default-node is not configured. Autopark is disabled.
```

```
Configuration node hierarchy

----------------------------

Config Node                 Type    Name

-----------                 ----    ----

/                           System

/md                         System

/md/campus                  Group

/md/campus/00:0b:86:9a:d5:d7  Device  demo-vpnc

/md/campus/00:0c:29:96:81:b3  Device  branch-vmc1

/mm                         System

/mm/mynode                  System

(demo-mm) [mynode] (config) #cd   branch-vmc1

(demo-mm) [00:0c:29:96:81:b3] (config) #masterip 10.1.101.10 vpn-ip 172.16.220.200 ipsec aruba123 peer-id 00:0B:86:9A:D5:D7 interface vlan 102

Change in the masterip configuration requires device to reload. Make sure the modified configuration ensures connectivity to the Master. Do you wan
t to continue [y/n]: y

(demo-mm) ^[00:0c:29:96:81:b3] (config) #write me

Saving Configuration...
```

```
Configuration Saved.
```

注意	针对两台 VPNC 的场景，我们仍然使用上述的一条 CLI，例如 masterip 10.1.101.10 vpn-ip 172.16.220.200 ipsec ****** peer-id 00:0B:86:9A:D5:D7 sec-peer-id 00:0B:86:9A:D5:D8 interface vlan 102 这里的 172.16.220.200 应该设计为 两台 VPNC 的 VRRP VIP 地址，采用 peer-id 后的 MAC 地址指向主 VPNC-1， sec-peer-id 后的 MAC 地址指向备 VPNC-2 ，此处使用的 MAC 地址必须为 VPNC 的 Management MAC Address 地址， 同时该 CLI 配置后会导致 Branch-MD 控制器需要重启一次才能生效。

Step3----在 VMM(本环境中的 Hostname=demo-mm)控制器上进行配置调整

```
在 Branch-MD 重启过程中，我们需要尽快在 Branch-MD 重启恢复前，完成下面的操作：

(demo-mm) [mm] (config) #show localip            （查看当前 VMM 控制器上存在两个 localip 白名单，分别指向每台 MD 控制器）

Local Switches configured by Local Switch IP

--------------------------------------------

Switch IP address of the Local  Key

-----------------------------  ---

172.16.220.200              ********

10.1.102.51                 ********
```

```
(demo-mm) [mm] (config) #show ip route      （查看 VMM 控制器上存在两条路由记录，分别指向两台 MD 控制器）

Codes: C - connected, O - OSPF, R - RIP, S - static, B - Bgw peer uplink

       M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN/Branch

       I - Ike-overlay, N - not redistributed


Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10

Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10

Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10

Gateway of last resort is 10.1.101.254 to network 0.0.0.0 at cost 1

S*    0.0.0.0/0  [0/1] via 10.1.101.254*

C    10.1.101.0/24 is directly connected, VLAN101

C    10.1.102.51/32 is an ipsec map          default-local-master-ipsecmap10.1.102.51

C    172.16.220.200/32 is an ipsec map     default-local-master-ipsecmap172.16.220.200



(demo-mm) [mm] (config) #no localip 10.1.102.51          （我们首先删除 角色被定为 Branch-MD 的白名单）
```

```
(demo-mm) ^[mm] (config) #write me

Saving Configuration...

Configuration Saved.

(demo-mm) [mm] (config) #show ip route                    （查看路由记录，只剩下到 角色被定义为 VPNC 的路由）

Codes: C - connected, O - OSPF, R - RIP, S - static, B - Bgw peer uplink

       M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN/Branch

       I - Ike-overlay, N - not redistributed


Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10

Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10

Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10

Gateway of last resort is 10.1.101.254 to network 0.0.0.0 at cost 1

S*    0.0.0.0/0  [0/1] via 10.1.101.254*

C    10.1.101.0/24 is directly connected, VLAN101

C    172.16.220.200/32 is an ipsec map default-local-master-ipsecmap172.16.220.200
```

```
(demo-mm) [mm] (config) #show switches            （此时的被定义为 Branch-MD 的控制器已经在 VMM 控制器上显示 down）

All Switches

------------

IP Address      IPv6 Address  Name        Location         Type    Model       Version       Status  Configuration State  Config Sync Time (sec)  Config ID

----------      ------------  ----        --------         ----    -----       -------       ------  -------------------  ----------------------  ---------

10.1.101.10     None          demo-mm     Building1.floor1  master  ArubaMM-VA  8.7.1.1_78245  up     UPDATE SUCCESSFUL    0                      5

172.16.220.200  None          demo-vpnc   Building1.floor1  MD      Aruba7010   8.7.1.1_78245  up     UPDATE SUCCESSFUL    0                      5

10.1.102.51     None          branch-vmc1  Building1.floor1  MD     ArubaMC-VA  8.7.1.1_78245  down   UPDATE REQUIRED      10                     4

Total Switches:3
```

当 Branch-MD 重启好后，在 VMM 上发现 Hostname=branch-vmc1 的控制器仍然 是 down 的状态：

```
(demo-mm) [mynode] #show switches

All Switches

------------

IP Address      IPv6 Address  Name        Location         Type    Model       Version       Status  Configuration State  Config Sync Time (sec)  Config ID
```

```
----------     ------------  ----       --------       ----    -----      -------      ------  ------------------  ---------------------  ---------

10.1.101.10     None        demo-mm     Building1.floor1  master  ArubaMM-VA  8.7.1.1_78245  up     UPDATE SUCCESSFUL    0                 7

172.16.220.200  None        demo-vpnc    Building1.floor1  MD      Aruba7010   8.7.1.1_78245  up     UPDATE SUCCESSFUL    0                 7

10.1.102.51     None        branch-vmc1  Building1.floor1  MD      ArubaMC-VA  8.7.1.1_78245  down    UPDATE REQUIRED     10                 4



Total Switches:3





(demo-mm) [mynode] #show running-config  | begin "ip route"     （在 VMM 控制器上发现 running-config 中多了一条到 Branch-MD 的静态路由配置）

Building Configuration...

ip route 10.1.102.51 255.255.255.255 ipsec  default-local-master-ipsecmap-00:0b:86:9a:d5:d7  20

ip nexthop-list load-balance-gateways

!

ip nexthop-list load-balance-ipsecs

!

ip nexthop-list traditional-ipsecs
```

```
!
```

而该路由条目并没有在路由表里激活，那是因为下一跳网关（default-local-master-ipsecmap-00:0b:86:9a:d5:d7）不存在。此时的VMM上，仅仅只有一条活跃的主机路由到VPNC(172.16.220.200)，并没有到Branch-MD（10.1.102.51）的隧道路由，这个就是导致MM和Branch-MD无法通讯的原因。

```
(demo-mm) [mynode] #show ip route

Codes: C - connected, O - OSPF, R - RIP, S - static, B - Bgw peer uplink

       M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN/Branch

       I - Ike-overlay, N - not redistributed



Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10

Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10

Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10

Gateway of last resort is 10.1.101.254 to network 0.0.0.0 at cost 1

S*    0.0.0.0/0  [0/1] via 10.1.101.254*

C    10.1.101.0/24 is directly connected, VLAN101

C    172.16.220.200/32 is an ipsec map     default-local-master-ipsecmap172.16.220.200
```

```
(demo-mm) [mynode] #show crypto  ipsec   ipsec-map-id

IPSEC MAP to ID mapping Information

-----------------------------------

Map Name                                        Map ID

--------                                     ------

default-local-master-ipsecmap172.16.220.200      0x4620
```

我们先到VMM系统上，须在/mm/mynode节点下，才能删除无用的到Branch-MD的主机静态路由（下一跳是基于MAC地址后缀的VPN网关—即VPNC）

```
(demo-mm) [mm] (config) #cd  /mm/mynode

(demo-mm) [mynode] (config) #no ip route 10.1.102.51 255.255.255.255  ipsec    default-local-master-ipsecmap-00:0b:86:9a:d5:d7

(demo-mm) ^[mynode] (config) #write me

Saving Configuration...

Configuration Saved.

(demo-mm) [mynode] (config) #
```

然后重新添加一条到Branch-MD的主机路由(下一跳是基于IP地址后缀的VPN网关—即VPNC）

```
(demo-mm) [mynode] (config) #show crypto ipsec ipsec-map-id

IPSEC MAP to ID mapping Information

-----------------------------------

Map Name                                        Map ID

--------                                   ------

default-local-master-ipsecmap172.16.220.200      0x4620


(demo-mm) [mynode] (config) #ip route 10.1.102.51 255.255.255.255 ipsec  default-local-master-ipsecmap172.16.220.200  20

Route will be added when the Ipsec Map default-local-master-ipsecmap172.16.220.200 is created

(demo-mm) ^[mynode] (config) #write me

Saving Configuration...

Configuration Saved.

(demo-mm) [mynode] (config) #


(demo-mm) [mynode] (config) #show ip route

Codes: C - connected, O - OSPF, R - RIP, S - static, B - Bgw peer uplink

     M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN/Branch
```

```
      I - Ike-overlay, N - not redistributed

Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10

Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10

Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10

Gateway of last resort is 10.1.101.254 to network 0.0.0.0 at cost 1

S*    0.0.0.0/0  [0/1] via 10.1.101.254*

S    10.1.102.51/32 [0/20] ipsec map       default-local-master-ipsecmap172.16.220.200       （到 Branch-MD 的路由条目）

C    10.1.101.0/24 is directly connected, VLAN101

C    172.16.220.200/32 is an ipsec map     default-local-master-ipsecmap172.16.220.200       （到 VPNC 的路由条目）
```

注意　你会发现，从 VMM 到 VPNC 和 Branch-MD 的两条路由条目，下一跳都是指向基于 IP 地址后缀的 VPN 网关—即 VPNC

Step4----查看相关状态，确保系统工作正常

经过前面的步骤后，你会发现 Branch-MD 的状态变更为 UP 了

```
(demo-mm) [mynode] (config) #show switches


All Switches

------------

IP Address      IPv6 Address  Name        Location         Type    Model      Version       Status  Configuration State  Config Sync Time (sec)  Config ID

----------      ------------  ----        --------         ----    -----      -------       ------  -------------------  ----------------------  ---------

10.1.101.10     None          demo-mm     Building1.floor1  master  ArubaMM-VA  8.7.1.1_78245  up     UPDATE SUCCESSFUL    0                  7

172.16.220.200  None          demo-vpnc   Building1.floor1  MD     Aruba7010   8.7.1.1_78245  up     UPDATE SUCCESSFUL    0                  7

10.1.102.51     None          branch-vmc1  Building1.floor1  MD     ArubaMC-VA  8.7.1.1_78245  up     UPDATE SUCCESSFUL    10                 7


Total Switches:3




(demo-mm) [mynode] (config) #show configuration node-hierarchy

Default-node is not configured. Autopark is disabled.

Configuration node hierarchy

----------------------------
```

```
Config Node                  Type    Name
-----------                  ----    ----
/                            System
/md                          System
/md/campus                   Group
/md/campus/00:0b:86:9a:d5:d7  Device   demo-vpnc
/md/campus/00:0c:29:96:81:b3  Device    branch-vmc1
/mm                          System
/mm/mynode                   System
```

在 VMM 控制器上，仅仅只有一个 IPSec 隧道到 VPNC。

```
(demo-mm) [mynode] #show crypto isakmp  sa
ISAKMP SA Active Session Information
------------------------------------
Initiator IP                 Responder IP                  Flags   Start Time      Private IP                    Peer ID
------------                 ------------                  -----   ----------      ----------                    -------------
```

```
172.16.220.200          10.1.101.10             r-v2-p   Feb  5 15:27:12    -                    IPV4_ADDR:172.16.220.200


Flags: i = Initiator; r = Responder

    m = Main Mode; a = Agressive Mode; v2 = IKEv2

    p = Pre-shared key; c = Certificate/RSA Signature; e =  ECDSA Signature

    x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled

    3 = 3rd party AP; C = Campus AP; R = RAP;  Ru = Custom Certificate RAP; I = IAP

    V = VIA; S = VIA over TCP; l = uplink load-balance

Total ISAKMP SAs: 1


在 VPNC 控制器上，有一个 IPSec 隧道到 VMM, 还有 另外一个隧道到 Branch-MD

(demo-vpnc) [MDC] #show crypto isakmp sa

ISAKMP SA Active Session Information

------------------------------------

Initiator IP           Responder IP            Flags   Start Time      Private IP                Peer ID

------------            ------------            -----   ----------      ----------                -------------

172.16.220.200          10.1.101.10             i-v2-p   Feb  5 15:10:28    -                    IPV4_ADDR:10.1.101.10
```

```
10.1.102.51          172.16.220.200         r-v2-p   Feb  5 16:50:30   -                 00:0c:29:96:81:a9


Flags: i = Initiator; r = Responder

    m = Main Mode; a = Agressive Mode; v2 = IKEv2

    p = Pre-shared key; c = Certificate/RSA Signature; e =  ECDSA Signature

    x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled

    3 = 3rd party AP; C = Campus AP; R = RAP;  Ru = Custom Certificate RAP; I = IAP

    V = VIA; S = VIA over TCP; l = uplink load-balance


Total ISAKMP SAs: 2




在 Branch-MD 控制器上，仅有一个 IPSec 隧道到 VPNC

(branch-vmc1) #show crypto isakmp sa

ISAKMP SA Active Session Information

------------------------------------

Initiator IP         Responder IP           Flags   Start Time     Private IP                Peer ID
```

```
------------             ------------             -----  ----------  ----------           -------------

10.1.102.51              172.16.220.200              i-v2-p   Feb  5 09:42:57   -                  00:0b:86:9a:d5:d7


Flags: i = Initiator; r = Responder

    m = Main Mode; a = Agressive Mode; v2 = IKEv2

    p = Pre-shared key; c = Certificate/RSA Signature; e =  ECDSA Signature

    x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled

    3 = 3rd party AP; C = Campus AP; R = RAP;  Ru = Custom Certificate RAP; I = IAP

    V = VIA; S = VIA over TCP; l = uplink load-balance


Total ISAKMP SAs: 1
```

注意

1）在该场景下，我们并没有去更改每台 MD 控制器所在的节点路径，仍然保持最初这些 MD 停靠的路径 /md/campus 下，仅仅是更改了 VMM，VPNC 和 Branch-MD 的配置，这样做的目的是为了减少由于设备更改节点路径而带来的重启过程（但是 Branch-MD 仍然是需要重启一次的），同时也减少了断网切割的时间。

2）当然，如果你是一个全新的安装环境，建议可以设计 VPNC 和 Branch-MD 分别属于不同的节点路径，配置上会更加清晰明了，不容易混淆节点路径而导致配置错误。

总结：

最后在整个配置变更过程中，VMM和VPNC都不需要硬件重启，仅仅实现配置变更就可以，而针对Branch-MD来说，必须要硬件重启一次，才能完成配置变更，需要相应的切割时间，需要和客户提前确定。

注意　上述配置例子中所用到的VMM，VPNC和Branch-MD的Management MAC Address ，IP地址和HW MAC Addr，请替换成你的环境中的相关地址。