aruba
a Hewlett Packard Enterprise company

MANAGED DEVICE AT BRANCH OFFICE (BOC)

Technical Climb Webinar

10:00 GMT | 11:00 CEST | 13:00 GST
Dec 19th, 2017

Presenter: Rajaguru Vincent

Rajaguru.Vincent@hpe.com

AIRHEADS COMMUNITY

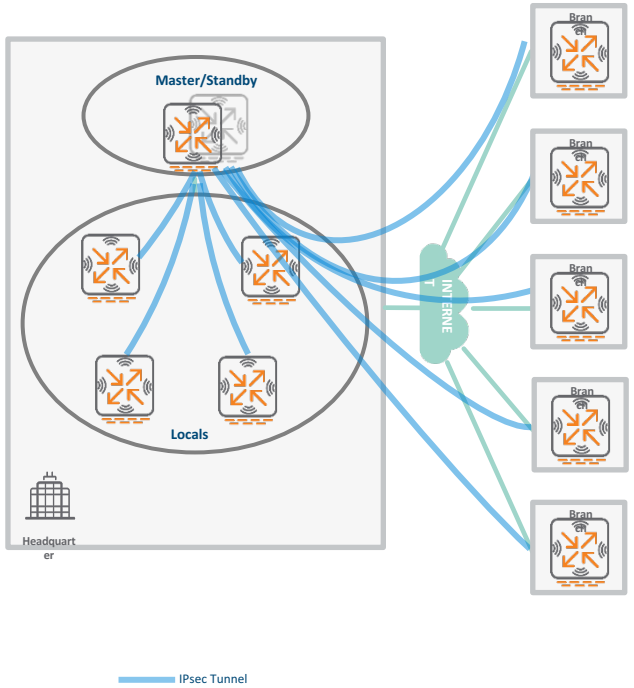
Branch Controller – A quick intro

What is a branch controller ? How it works?

- Branch controllers enable customers to directly plug the controller into a broadband internet modem and establish communication to Master controller in the corporate data centers
- From behind an internet mode, Branch controller reaches the Master controller just like a RAP or an IAP VPN.
- Branch controllers are designed for small to medium-scale where only 1-64 APs are required
- Branch controller finds the Master by static configuration or ZTP.
- All configuration of the Branch controller including VLAN creation are done from the Master controller or MM.

Branch Office Deployment in 6.x

1. IPsec of BOC always terminates on Master controller
2. ZTP supported via Activate server
3. BOC whitelist can be manually added in the master
4. BOC configurations are made through Smart Config Wizard

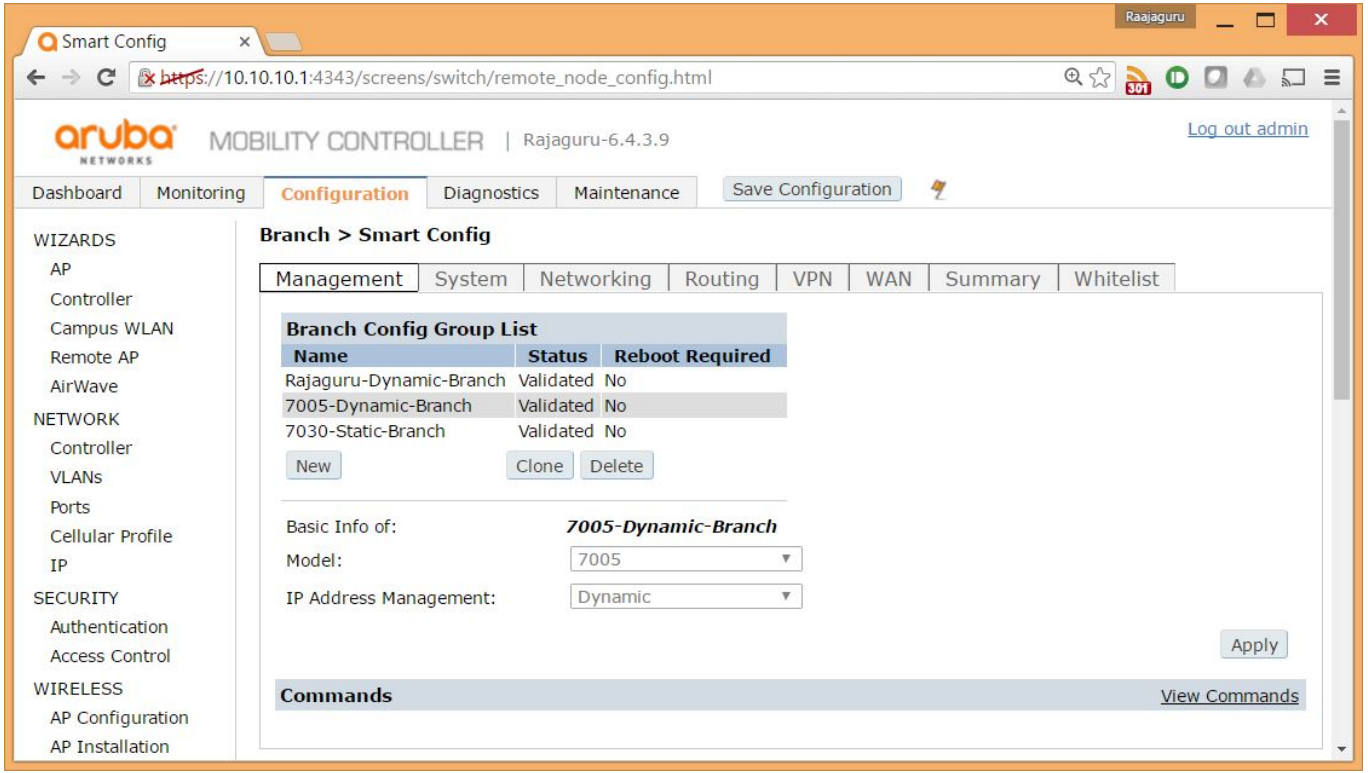


Branch deployment 6.x - Manual (full-setup)

```
Auto-provisioning is in progress. Choose one of the following options to override or debug...
   'enable-debug'  : Enable auto-provisioning debug logs
   'disable-debug' : Disable auto-provisioning debug logs
   'mini-setup'    : Stop auto-provisioning and start mini setup dialog for branch role
   'full-setup'    : Stop auto-provisioning and start full setup dialog for any role


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
Enter System name [Aruba7005]:       branch01-7005
Enter Switch Role (master|local|standalone|branch) [master]:        branch
Enter Branch Master switch IP address or FQDN [172.16.0.254]:          10.69.129.100
Enter Branch wired uplink port [GE 0/0/0]:        GE 0/0/3
Enter Branch wired-vlan Type (pppoe|dhcp|static) [static]:        dhcp
This controller is restricted to Country code US for United States, please confirm?:          yes
Enter Time Zone [PST-8:0]:
Enter Time in UTC [00:24:38]:
Enter Date (MM/DD/YYYY) [5/5/2015]:
```

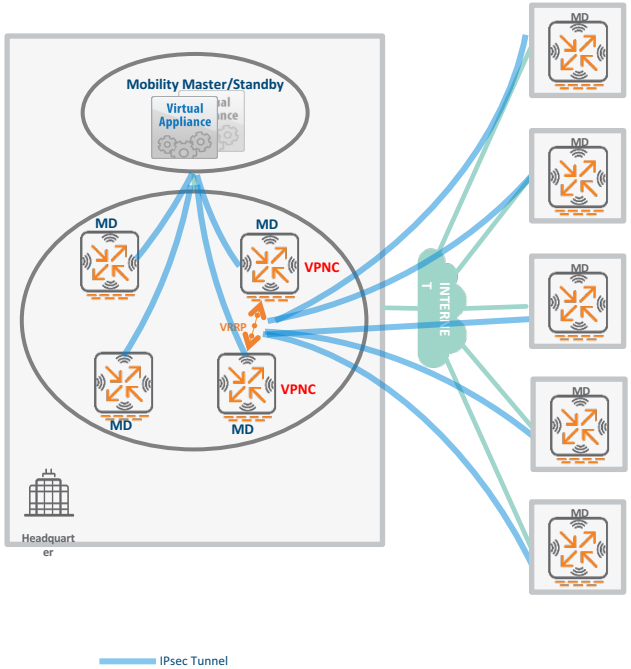
Smart Config in 6.x



Branch Office Deployment in 8.x

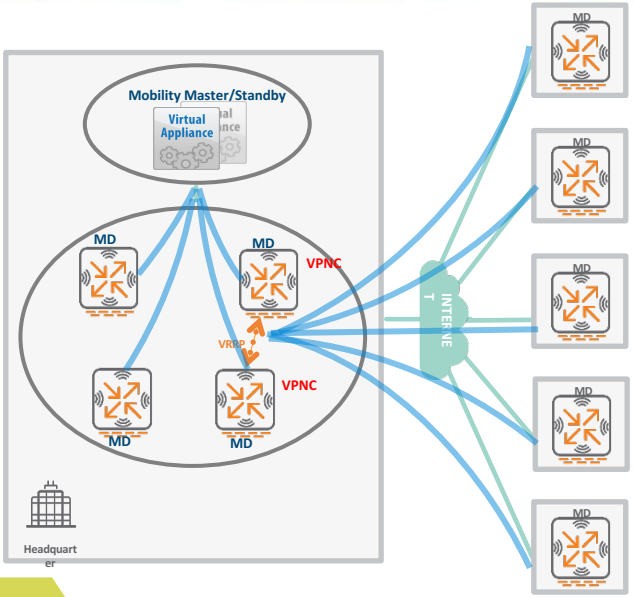
- VPN Concentrator -- VPNC

1. MM manages all the MDs in the network
2. One or a pair of MDs as VPNC to terminate branch office controller IPsec
3. Multiple Branch office controllers establishe IPsec tunnel to VPNC
4. Only one IPsec tunnel from the VPNC to MM
5. BOC in 8.x is just an MD and configuration are made at node level



BOC Initial setup in 8.x

```
Enter System name [Aruba7030]:
Enter Switch Role (master|standalone|md) [md]: md
Enter IP type to terminate IPSec tunnel (ipv4|ipv6) [ipv4]:
Enter Master switch IP address or FQDN: 10.70.92.5
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]: yes
Enter VPN concentrator IP address:      10.70.92.15
VPN concentrator Authentication method (FactoryCert|PSKwithMAC)
 [FactoryCert]:
Enter VPN concentrator MAC address:     00:0B:86:B5:88:67
Enter Redundant VPN concentrator MAC address [none]:
 00:0B:86:B5:87:77
```



VPNC is a MD which can terminate IPsec tunnels from other MDs.

IPsec Tunnel

ADD THE MAC ADDRESS OF THE BOC ON THE VPN CONC:

```
[mynode] (config) #cd /md/VPN-Con-Group
[VPN-Con-Group] (config) #vpn-peer peer-mac 00:0b:86:bc:03:27 cert-auth factory-cert
```

ZTP – Zero Touch Provisioning for a MD

This method requires interactions of MD with activate server to get MM information.

User has to configure Activate credentials on MM for ZTP to work. MM uses it to register itself and upload its certificate on Activate.

```
(ArubaMM) [mm] #show activate

activate
--------
Parameter                                 Value                                 Set
---------                                 -----                                 ---
Activate Whitelist Service                Enabled
Activate URL                              https://activate.arubanetworks.com
Provision Activate URL                    https://device.arubanetworks.com
Activate Login Username                   apingale
Activate Login Password                   ********
Periodic Interval for WhiteList Download  1
Add-Only Operation                        Enabled
Custom cert to upload to Activate         CustomCACert
Server cert to be used for IPSEC          CustomServerCert
```

You will have to connect last copper port of Branch Controller as Uplink for controller which will have vlan 4094 configured with dhcp client working on it.

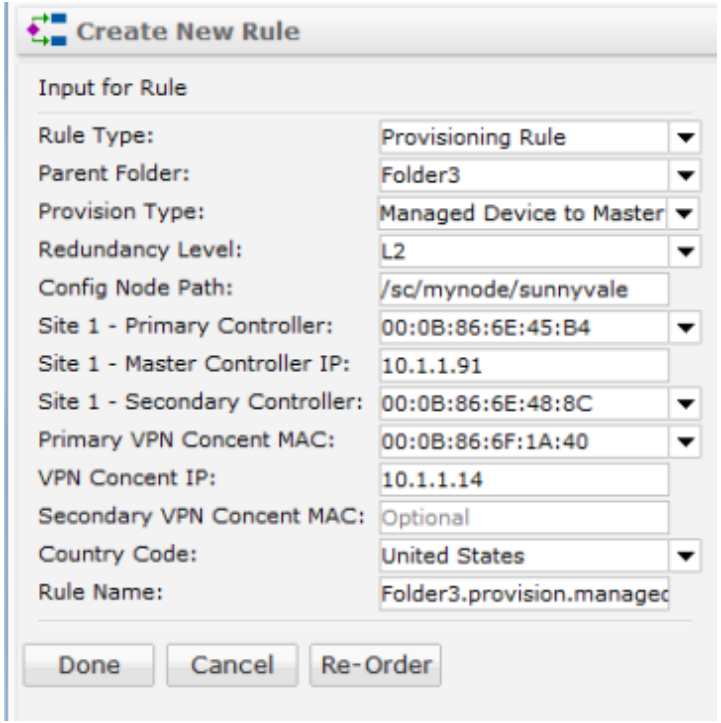
- **MD establishes HTTPS connection with the activate server (device.arubanetworks.com) and posts provision request to it.**
- **Activate server authenticates the controller and on successful authentication provides MM information, Country Code to the MD and downloads Trust Anchor to MD.**

ZTP – Zero Touch Provisioning for a MD

- **You will have to connect last copper port of Branch Controller as Uplink for controller which will have vlan 4094 configured with dhcp client working on it.**
- **MD establishes HTTPS connection with the activate server (device.arubanetworks.com) and posts provision request to it.**
- **Activate server authenticates the controller and on successful authentication provides MM information, Country Code to the MD and downloads Trust Anchor to MD.**
- **Branch MD establishes IPSec with VPNC and connects with MM through MD-VPNC IPSec.**
- **MD establishing connection with MM through VPNC is supported only with Factoty-certs on VPNC and MD.**
- **MM will have reverse route to MD through VPNC-MM IPSec which will be installed automatically.**
- **VPNC will have PSK based IPSec tunnel with MM. VPNC will be added to activate Manually.**
- **Command below will be added to VPNC automatically:**

```
vpn-peer peer-mac "00:0b:86:bf:83:d0" cert-auth factory-cert
```

Activate Configuration



Debugging

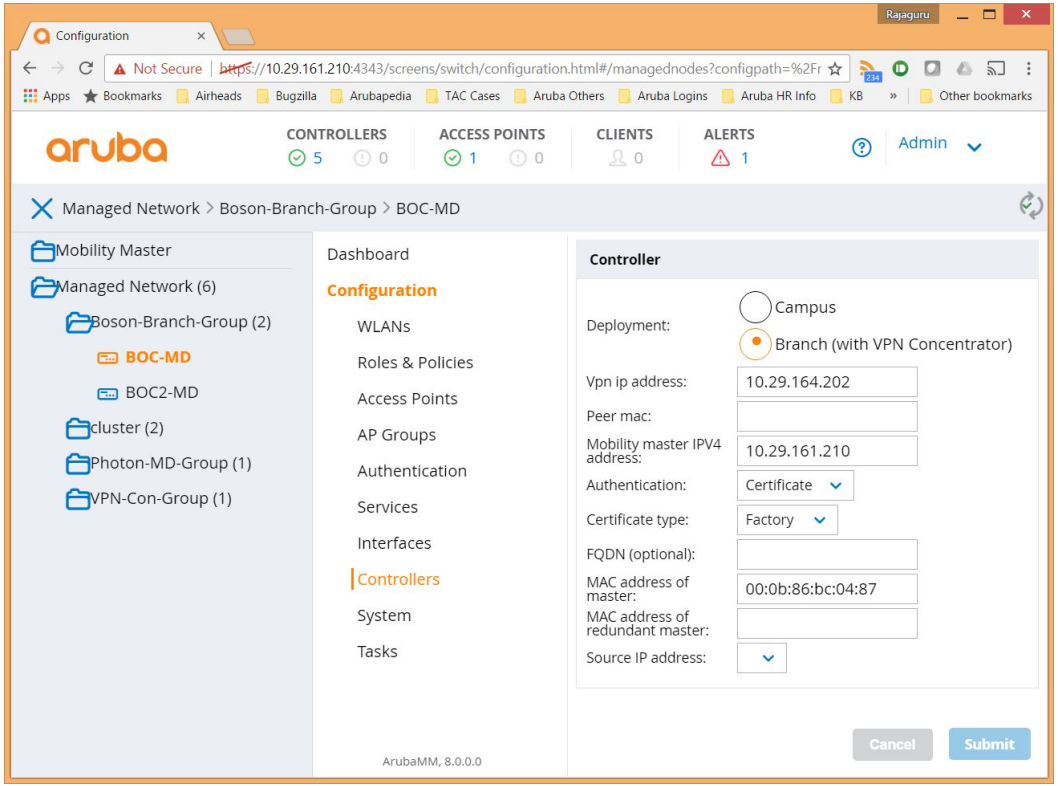
Commands to see Status of MD on MM:

- `Show crypto isakmp sa`
- `Show crypto ipsec sa`
- `Show switches`

For debugging IPSec issues use debugging levels below:

- `Logging level debugging security`
- `Logging level debugging security process crypto subcat ike`
- `Show log security all`
- `Logging level debugging system process bocmgr`
- `Logging level debugging system process cpsec`
- `Show log system all`

Branch Controller Configuration in 8.0



8.X FEATURES FOR BRANCH

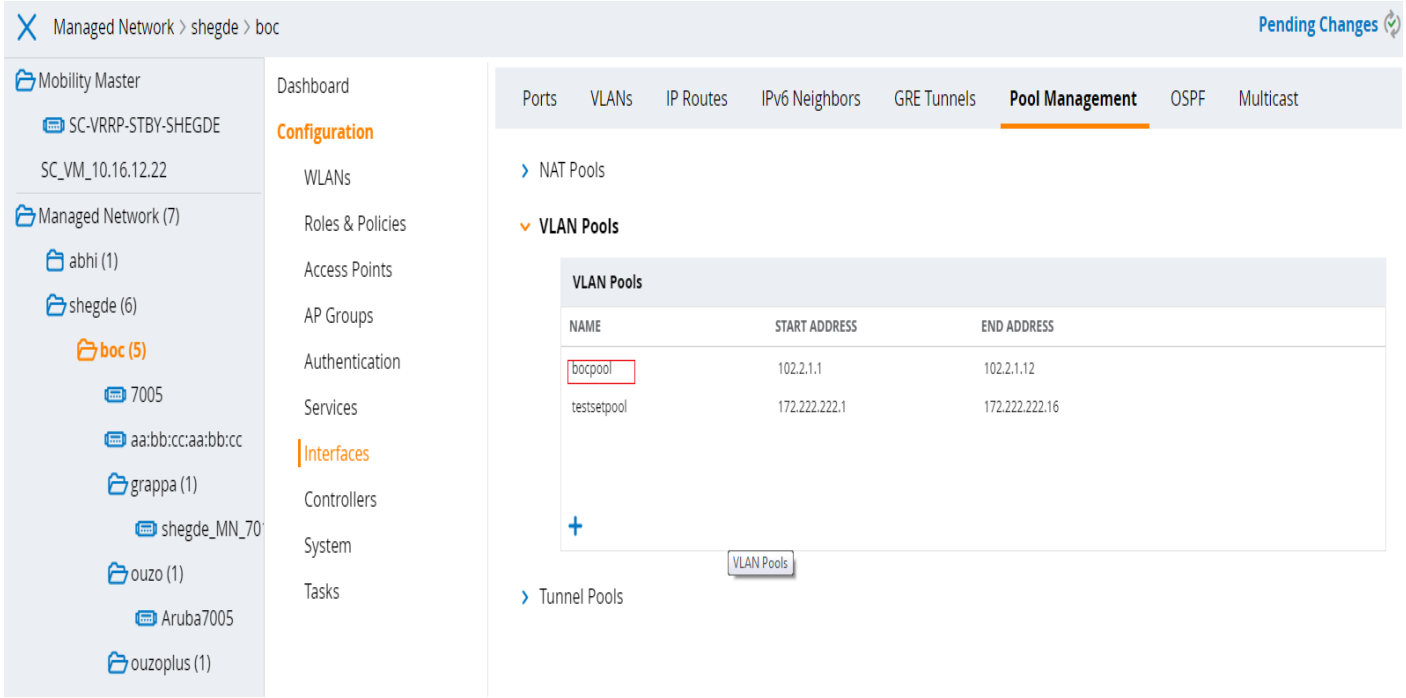
aruba
a Hewlett Packard
Enterprise company

Address Pool Management and Pool carving

- IP Address Pools are used for Dynamic IP address carving for,
  - VLAN pool
  - TUNNEL pool
  - NAT pool
  - DHCP pool
- Pool config can be added at node level .
- Pool needs to be assigned to an interface for it to take effect
- Pool carving comes into effect when a device is added under the node
- Each device under node will get its IP's /subnet carved dynamically
- Deletion of device free up the ips and gets added back to pool
- Device addition is prevented if there are no free IP in the pool

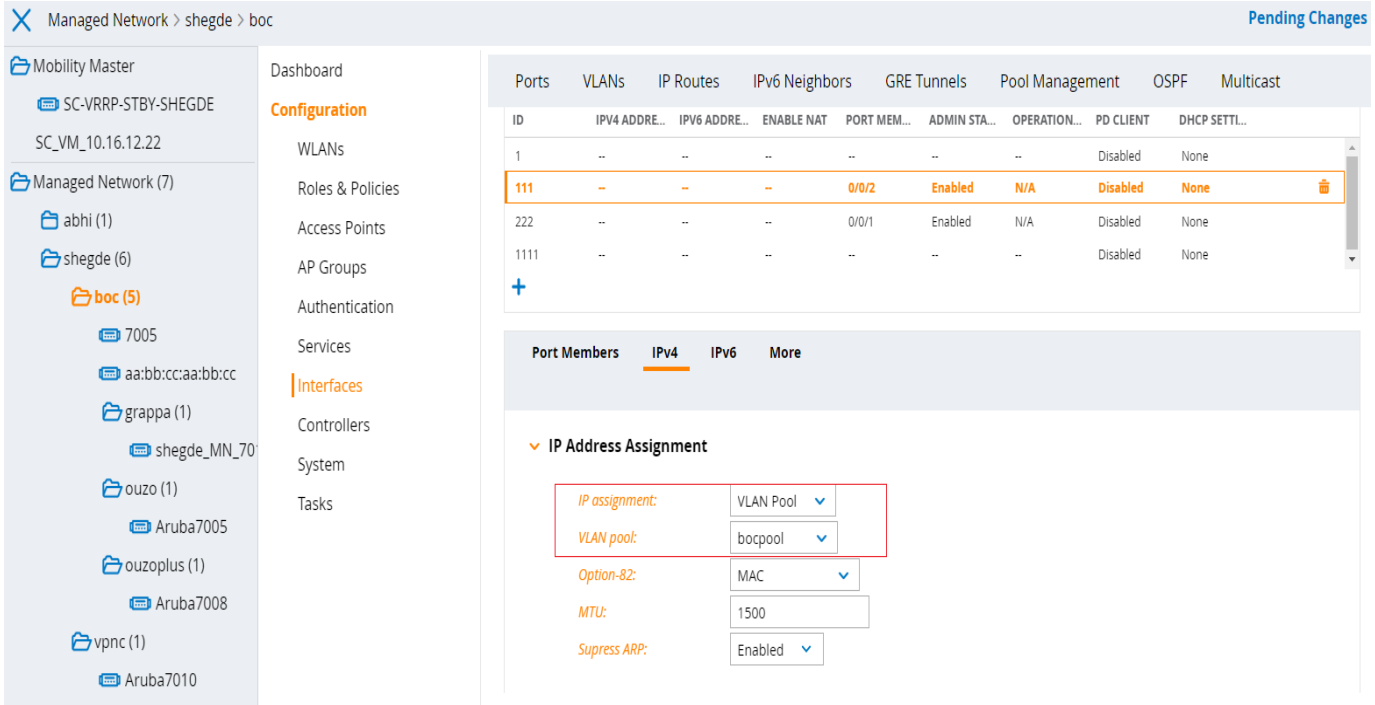
VLAN Pool configuration

Configuration -> interfaces -> pool management



VLAN Pool Assignment

- Assigning VLAN POOL to interface vlan under configurations->interfaces->vlan



Pool reference check using bocmgr in MM

- VLAN Pool reference details

```
(SC_VM_10.16.12.22) [boc] (config-submode)#show bocmgr pool vlan pool-name bocpool

Vlan Pool(s)
------------
Pool Name  Vlan Id  Start IP   End IP     Next IP  Number of Hosts Intf ref count DeviceRefcount PoolNode
---------  -------  --------   ------     -------  --------------- -------------- --------------  ---------
bocpool    111      102.2.1.1  102.2.1.12   0                              1            5     /md/shegde/boc
```

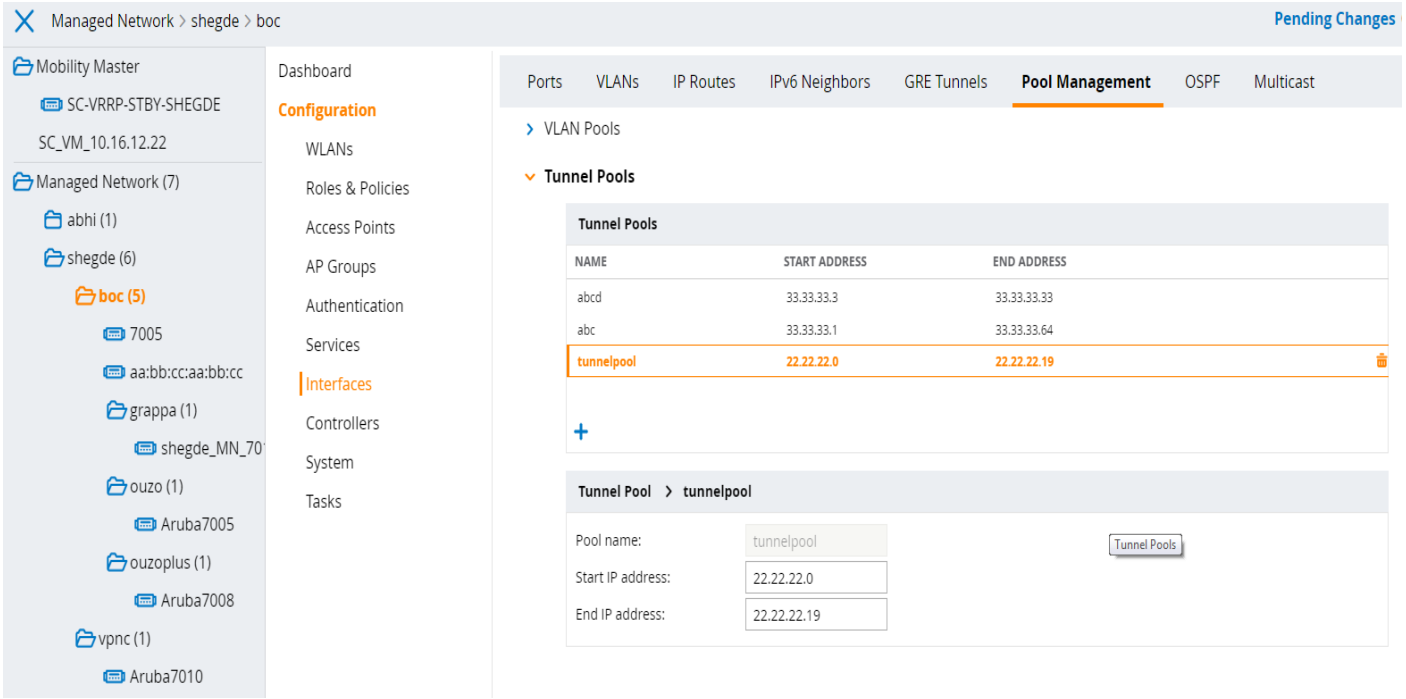
- Interface reference count is 1 , since its assigned only to vlan 111
- 5 devices exist under node level /md/shegde/boc . Hence total device reference is 5

- VLAN IP Assignment to BOC

```
(shegde_MN_7010) #show configuration effective | begin "interface vlan 111"
interface vlan 111
    ip address 102.2.1.1 255.255.255.255
    description test
!
```

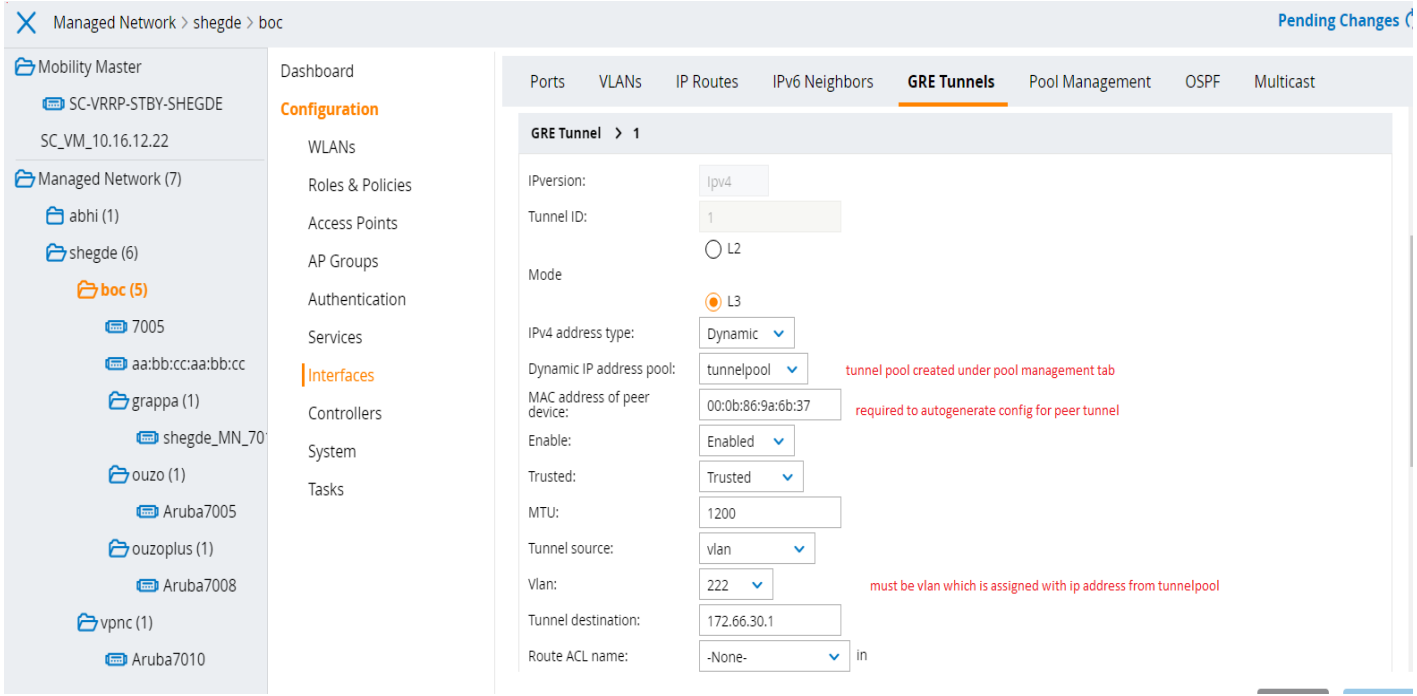
Tunnel Pool Configuration

- Configuring Tunnel Pool



Tunnel Pool assignment to GRE tunnel

- Configuration -> interfaces -> GRE tunnels



L3 GRE tunnel – Autogenerated tunnel interfaces

Peer IP autogenerated at boc/md

```
(shegde_MN_7010) #show interface tunnel 1

Tunnel 1 is up line protocol is up
Description: Tunnel Interface
Internet address is 22.22.22.5 255.255.255.252
Source  172.16.222.65 (Vlan 222)
Destination 172.66.30.1
Tunnel mtu is set to 1500
Tunnel is an IP GRE TUNNEL
Tunnel is Trusted
Inter Tunnel Flooding is enabled
Tunnel keepalive is enabled
Keepalive type is Default
Tunnel keepalive interval is 10 seconds, retries 3
        Heartbeats sent 2, Heartbeats lost 1
        Tunnel is down 2 times
Rx access list -None- is configured
```

Autogenerated peer tunnel config at destination VPNC

```
(Aruba7010) #show interface tunnel 64001
Tunnel 64001 is up line protocol is down
Description: Tunnel Interface
Internet address is 22.22.22.6 255.255.255.252
Source  172.66.30.1
Destination 172.16.222.65
Tunnel mtu is set to 1500
Tunnel is an IP GRE TUNNEL
Tunnel is Trusted
Inter Tunnel Flooding is enabled
OSPF is enabled on this interface
Tunnel keepalive is enabled
Keepalive type is Default
Tunnel keepalive interval is 10 seconds, retries 3
        Heartbeats sent 51, Heartbeats lost 50
        Tunnel is down 3 times
```

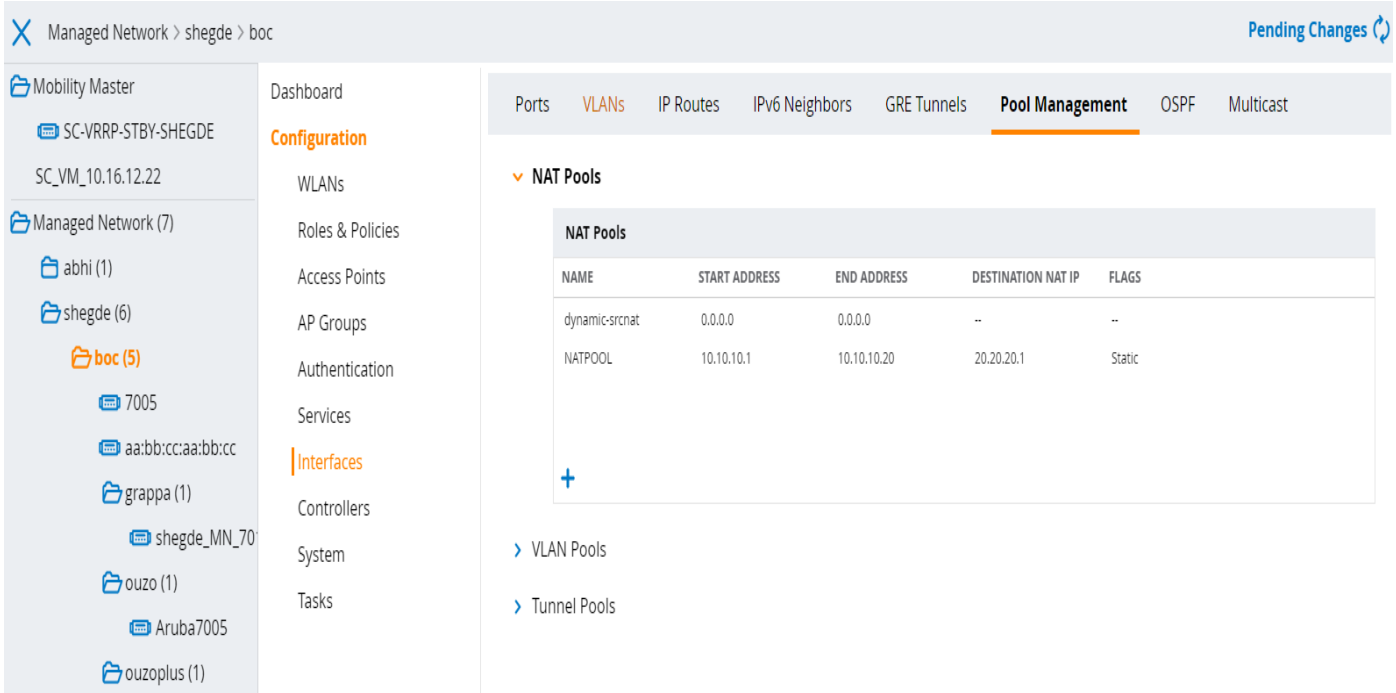
Tunnel pool reference details

```
(SC_VM_10.16.12.22) [boc] (config) #show bocmgr pool tunnel pool-name tunnelpool

Tunnel Pool(s)
Pool Name   Tunnel Id  Start IP    End IP      Next IP  Number of Hosts  Intf ref count  Device ref count  Pool Node      Autogen  PeerDev
---------   ---------  --------    ------      -------  ---------------  --------------  ----------------  ---------      -------  -----------
tunnelpool  1          22.22.22.0  22.22.22.19          1                1               5                 /md/shegde/boc true   00:0b:86:9a:6b:37
```

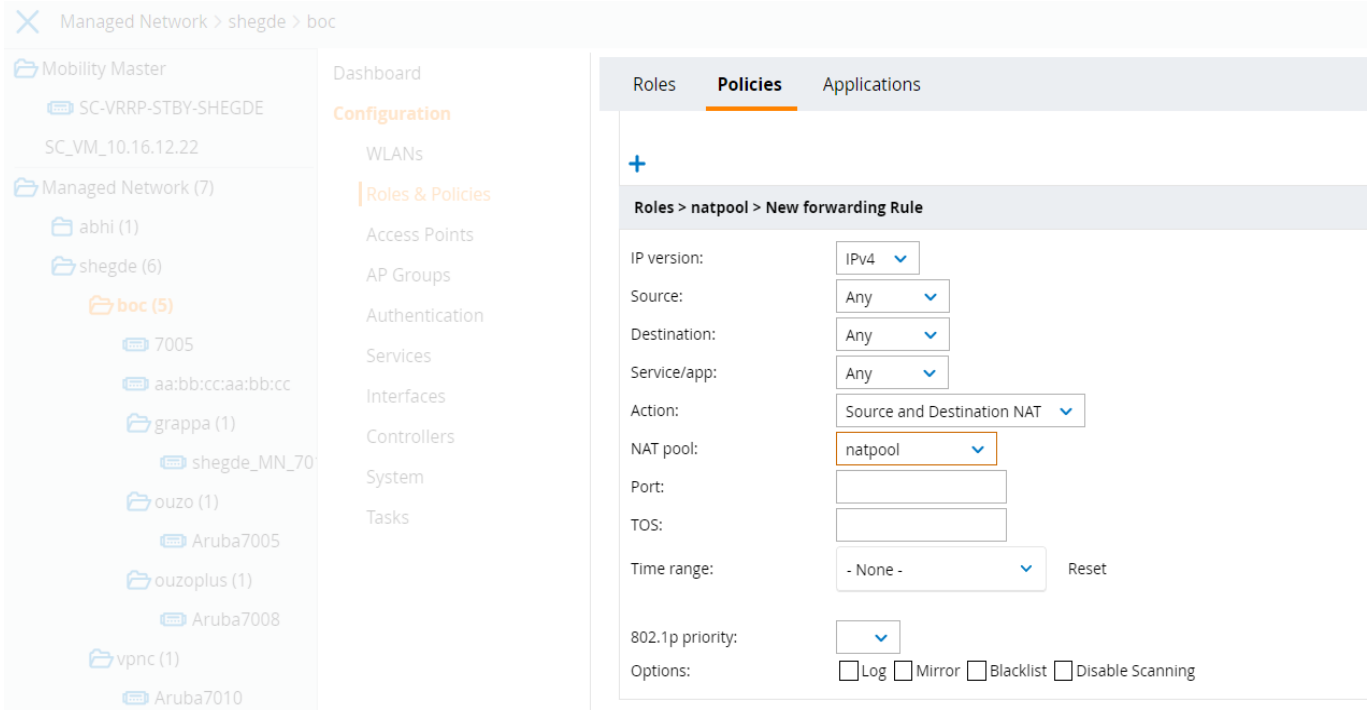
NAT Pool

- NAT POOL configuration



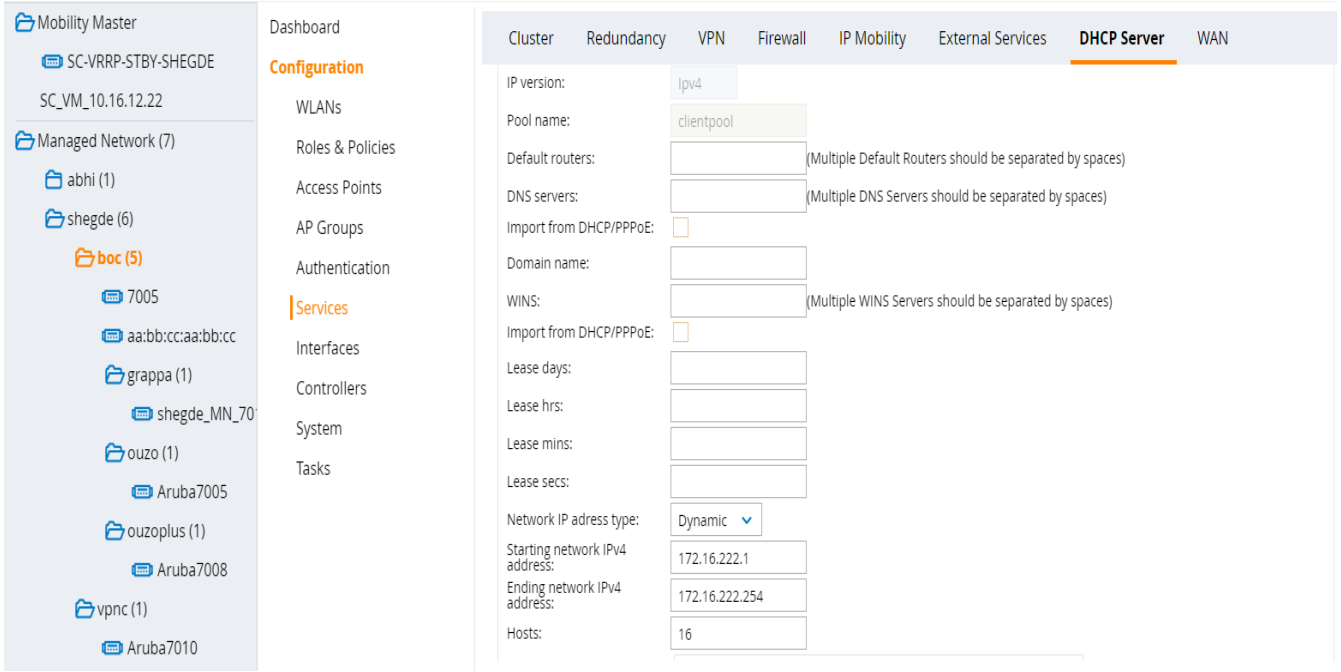
NAT Pool

- NAT POOL configuration in session ACL



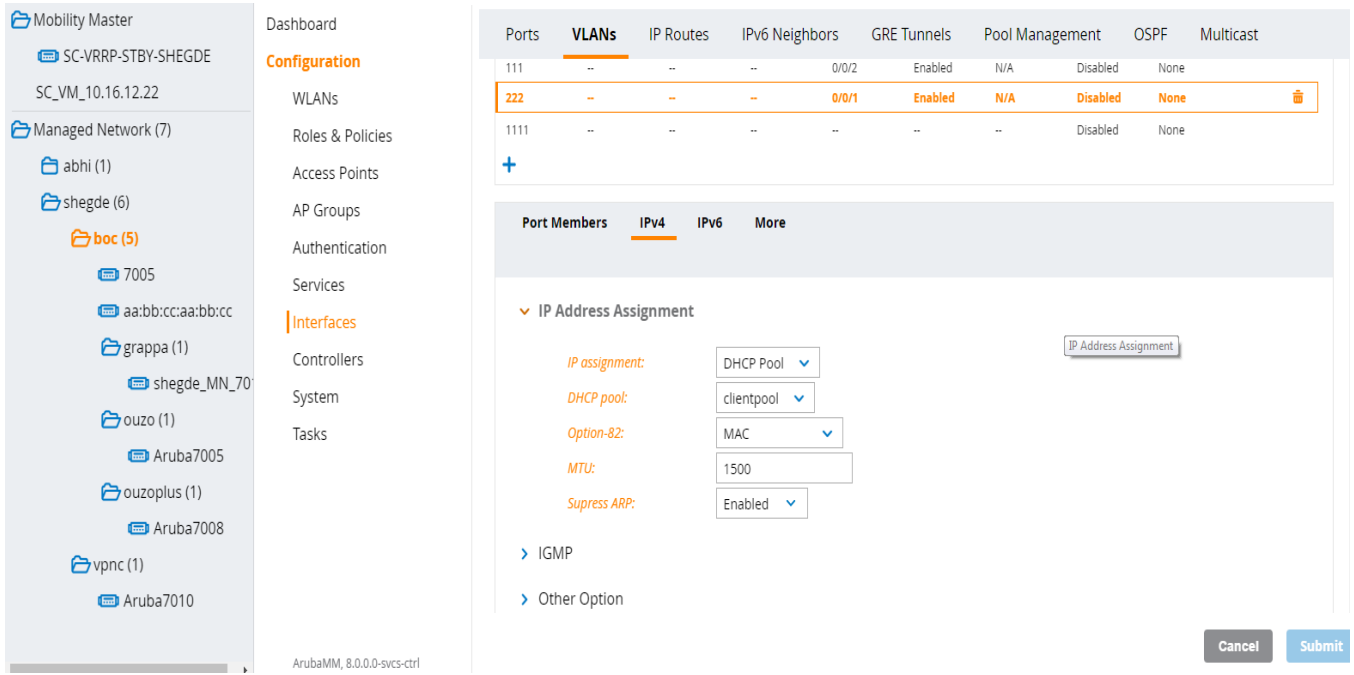
DHCP Pool Configuration

- Configuration -> services -> dhcp server



DHCP Pool Assignment

- Configuration -> interfaces -> VLAN



DHCP Pool Carving

- DHCP Pool Carving

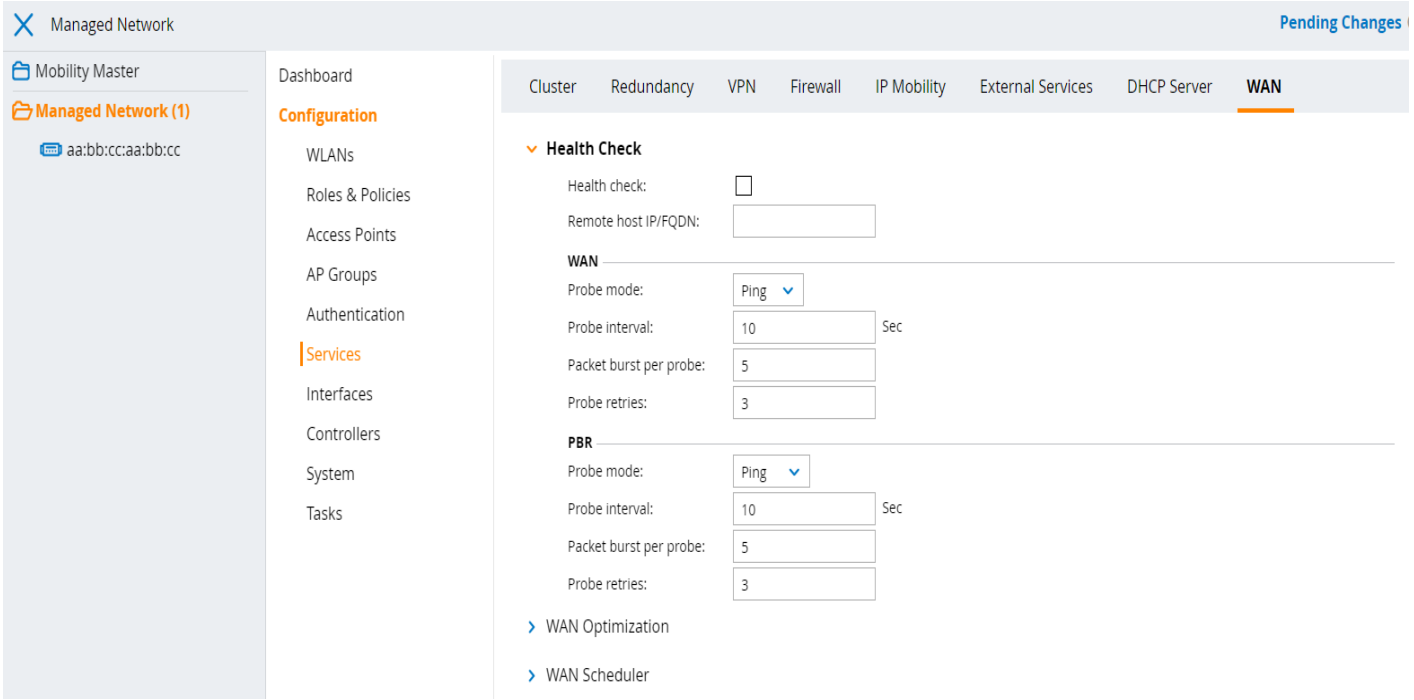
IP address Range : 192.168.23.1 - 192.168.23.254 with 16 to 30 hosts will be carved into eight networks as below

Example 16 to 30 hosts:

- Network 192.168.23.0 /27 First IP 192.168.23.1
- Network 192.168.23.32 /27 First IP 192.168.23.33
- Network 192.168.23.64 /27 First IP 192.168.23.65
- Network 192.168.23.96 /27 First IP 192.168.23.97
- Network 192.168.23.128 /27 First IP 192.168.23.129
- Network 192.168.23.160 /27 First IP 192.168.23.161
- Network 192.168.23.192 /27 First IP 192.168.23.193
- Network 192.168.23.224 /27 First IP 192.168.23.225

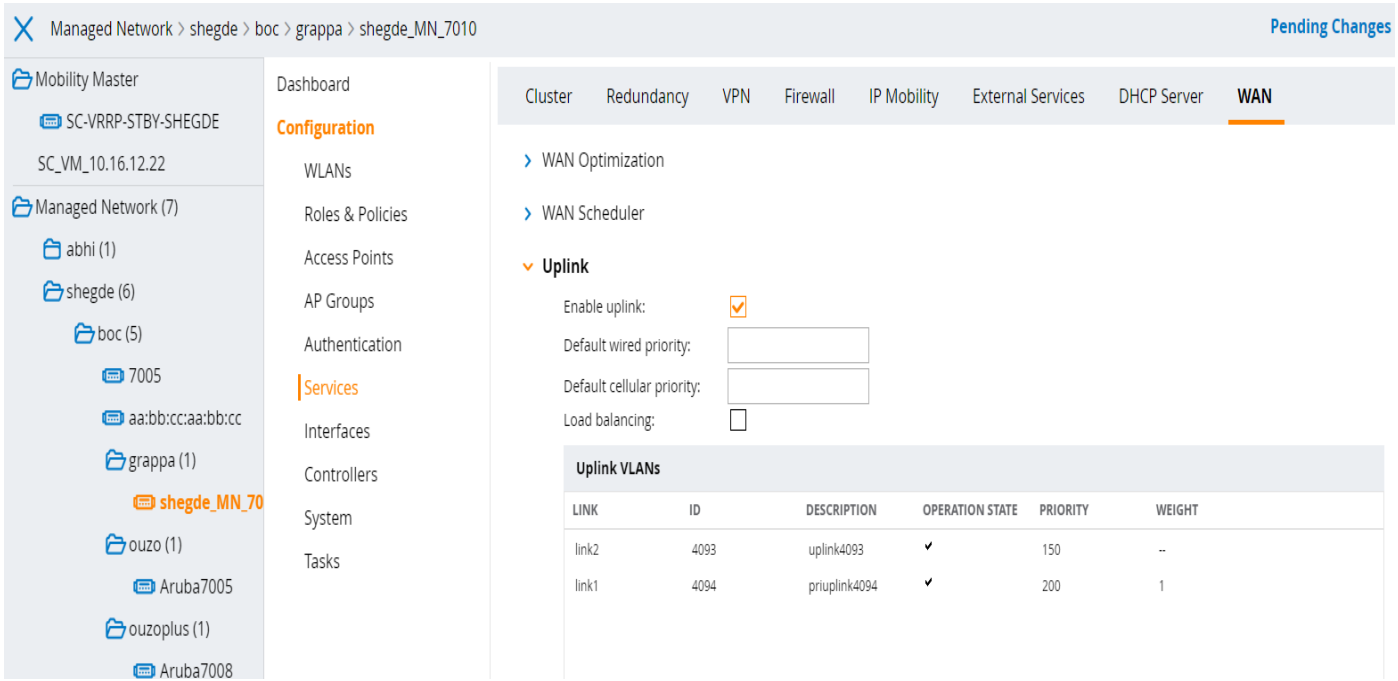
WAN health check config

- Configuration->services->WAN



Configuring WAN uplinks

- Configuration -> services -> WAN -> uplink

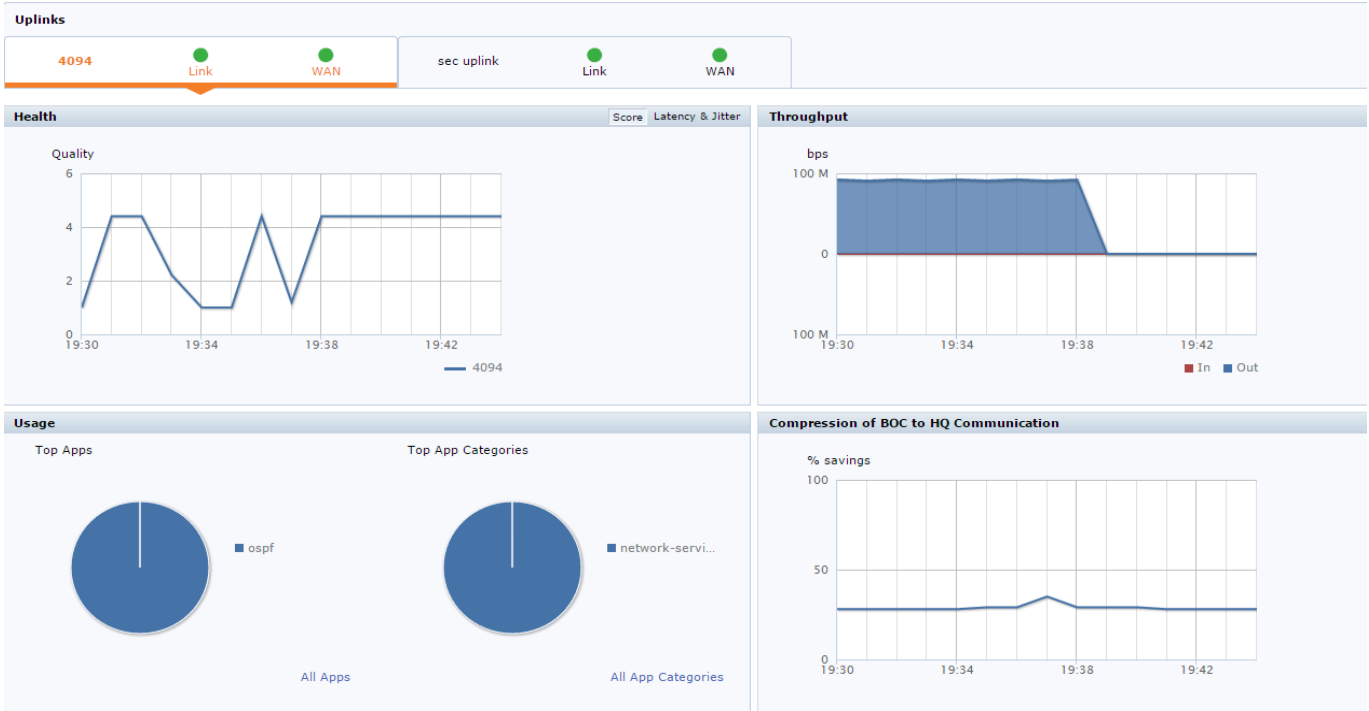


Checking WAN uplink status

```
(host) #show uplink
Uplink Manager: Disabled
Uplink Health-check: Enabled
Uplink Health-check IP/FQDN: 192.0.2.14
Uplink Management Table
-----------------------
Id  Uplink Type  Properties     Priority  State      Status      Reachability
--  -----------  ----------     --------  -----      ------      ------------
1   Wired        vlan 4094      200       Connected  Active      Reachable
2   Cellular     Novatel_U727   100       Standby    Ready       Reachable
```

WAN Dashboard

- BOC's WAN Dashboard



THANK YOU

aruba
a Hewlett Packard
Enterprise company