

# 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



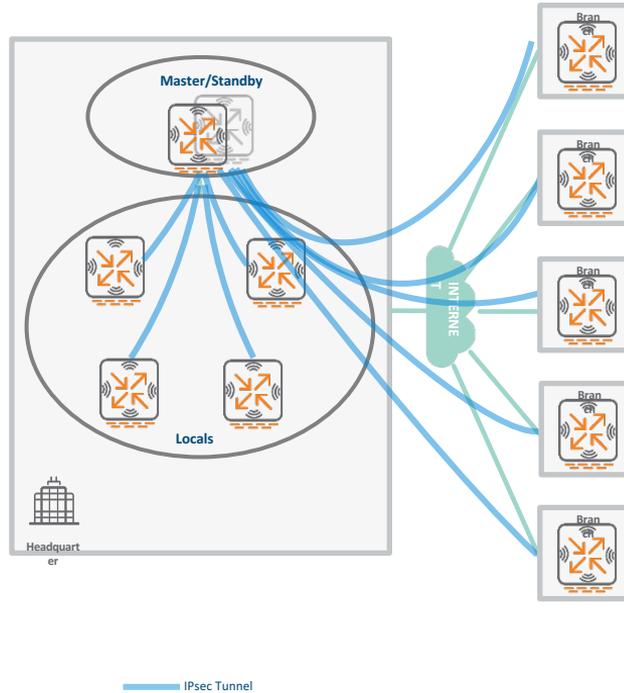
# Branch Controller – A quick intro

## 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

The screenshot shows the Aruba Mobility Controller web interface. The browser address bar displays `https://10.10.10.1:4343/screens/switch/remote_node_config.html`. The page title is "MOBILITY CONTROLLER | Rajaguru-6.4.3.9". The navigation menu includes "Dashboard", "Monitoring", "Configuration", "Diagnostics", and "Maintenance". A "Save Configuration" button is visible. The left sidebar lists various configuration categories: WIZARDS (AP, Controller, Campus WLAN, Remote AP, AirWave), NETWORK (Controller, VLANs, Ports, Cellular Profile, IP), SECURITY (Authentication, Access Control), and WIRELESS (AP Configuration, AP Installation). The main content area is titled "Branch > Smart Config" and has tabs for "Management", "System", "Networking", "Routing", "VPN", "WAN", "Summary", and "Whitelist". The "Management" tab is active, showing a "Branch Config Group List" table with columns for Name, Status, and Reboot Required. The table lists three entries: "Rajaguru-Dynamic-Branch", "7005-Dynamic-Branch", and "7030-Static-Branch", all with a status of "Validated" and "No" for "Reboot Required". Below the table are "New", "Clone", and "Delete" buttons. The "Basic Info of:" section for the selected "7005-Dynamic-Branch" shows "Model:" set to "7005" and "IP Address Management:" set to "Dynamic". An "Apply" button is located at the bottom right of this section. A "Commands" section at the bottom has a "View Commands" link.

Aruba NETWORKS MOBILITY CONTROLLER | Rajaguru-6.4.3.9 [Log out admin](#)

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
AP  
Controller  
Campus WLAN  
Remote AP  
AirWave  
NETWORK  
Controller  
VLANs  
Ports  
Cellular Profile  
IP  
SECURITY  
Authentication  
Access Control  
WIRELESS  
AP Configuration  
AP Installation

**Branch > Smart Config**

Management System Networking Routing VPN WAN Summary Whitelist

**Branch Config Group List**

Name	Status	Reboot Required
Rajaguru-Dynamic-Branch	Validated	No
7005-Dynamic-Branch	Validated	No
7030-Static-Branch	Validated	No

New Clone Delete

Basic Info of: **7005-Dynamic-Branch**

Model: 7005

IP Address Management: Dynamic

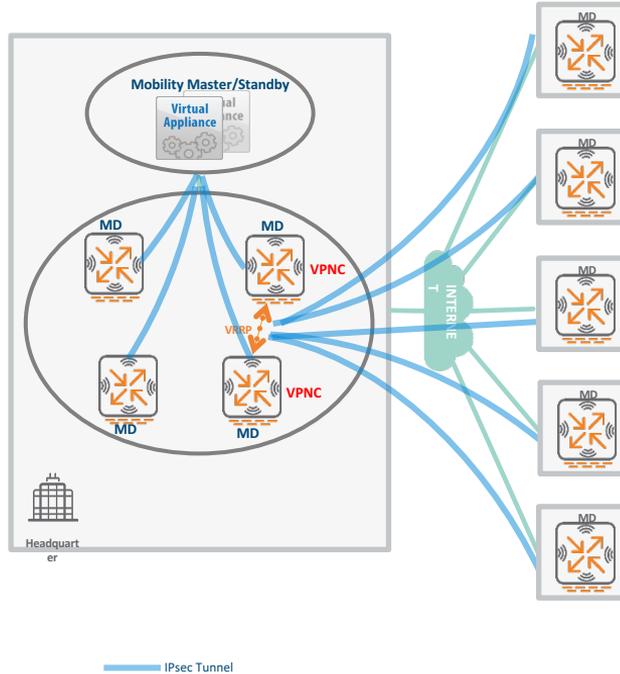
Apply

Commands [View Commands](#)

# 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 establish 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



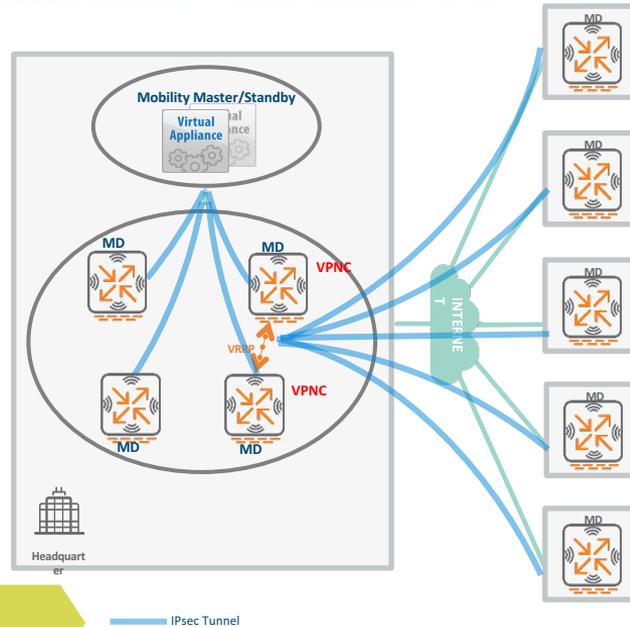
# BOC Initial setup in 8.x

```
1 MM not optimized for bulk IPsec
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.

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 Factory-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

 **Create New Rule**

Input for Rule

Rule Type:	Provisioning Rule	▼
Parent Folder:	Folder3	▼
Provision Type:	Managed Device to Master	▼
Redundancy Level:	L2	▼
Config Node Path:	/sc/mynode/sunnyvale	
Site 1 - Primary Controller:	00:0B:86:6E:45:B4	▼
Site 1 - Master Controller IP:	10.1.1.91	
Site 1 - Secondary Controller:	00:0B:86:6E:48:8C	▼
Primary VPN Concent MAC:	00:0B:86:6F:1A:40	▼
VPN Concent IP:	10.1.1.14	
Secondary VPN Concent MAC:	Optional	
Country Code:	United States	▼
Rule Name:	Folder3.provision.managed	

# 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

The screenshot displays the Aruba Configuration web interface. At the top, the browser address bar shows the URL: `https://10.29.161.210:4343/screens/switch/configuration.html#/managednodes?configpath=%2Fr`. The interface includes a navigation menu on the left with the following items: Mobility Master, Managed Network (6), Boson-Branch-Group (2), BOC-MD (selected), BOC2-MD, cluster (2), Photon-MD-Group (1), and VPN-Con-Group (1). The main content area is titled "Controller" and features the following configuration options:

- Deployment:  Campus,  Branch (with VPN Concentrator)
- Vpn ip address:
- Peer mac:
- Mobility master IPV4 address:
- Authentication:
- Certificate type:
- FQDN (optional):
- MAC address of master:
- MAC address of redundant master:
- Source IP address:

At the bottom of the configuration panel, there are "Cancel" and "Submit" buttons. The footer of the interface indicates the version: "ArubaMM, 8.0.0.0".

# 8.X FEATURES FOR BRANCH

# 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

Managed Network > shegde > boc Pending Changes

Mobility Master

- SC-VRRP-STBY-SHEGDE
- SC\_VM\_10.16.12.22

Managed Network (7)

- abhi (1)
- shegde (6)
  - boc (5)**
    - 7005
    - aa:bb:cc:aa:bb:cc
    - grappa (1)
    - shegde\_MN\_70
    - ouzo (1)
    - Aruba7005
    - ouzoplus (1)

Dashboard

**Configuration**

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces**
- Controllers
- System
- Tasks

Ports VLANs IP Routes IPv6 Neighbors GRE Tunnels **Pool Management** OSPF Multicast

> NAT Pools

▼ **VLAN Pools**

VLAN Pools		
NAME	START ADDRESS	END ADDRESS
bocpool	102.2.1.1	102.2.1.12
testsetpool	172.222.222.1	172.222.222.16

+  
VLAN Pools

> Tunnel Pools

# VLAN Pool Assignment

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

Managed Network > shegde > boc Pending Changes

Mobility Master  
SC-VRRP-STBY-SHEGDE  
SC\_VM\_10.16.12.22

Managed Network (7)  
abhi (1)  
shegde (6)  
    **boc (5)**  
        7005  
        aa:bb:cc:aa:bb:cc  
        grappa (1)  
        shegde\_MN\_70  
        ouzo (1)  
        Aruba7005  
        ouzoplus (1)  
        Aruba7008  
vpnc (1)  
    Aruba7010

Dashboard  
**Configuration**  
WLANs  
Roles & Policies  
Access Points  
AP Groups  
Authentication  
Services  
**Interfaces**  
Controllers  
System  
Tasks

Ports	VLANs	IP Routes	IPv6 Neighbors	GRE Tunnels	Pool Management	OSPF	Multicast	
ID	IPv4 ADDRE...	IPv6 ADDRE...	ENABLE NAT	PORT MEM...	ADMIN STA...	OPERATION...	PD CLIENT	DHCP SETTL...
1	--	--	--	--	--	--	Disabled	None
111	--	--	--	0/0/2	Enabled	N/A	Disabled	None
222	--	--	--	0/0/1	Enabled	N/A	Disabled	None
1111	--	--	--	--	--	--	Disabled	None

**Port Members** | IPv4 | IPv6 | More

**IP Address Assignment**

IP assignment:	VLAN Pool
VLAN pool:	bocpool
Option-82:	MAC
MTU:	1500
Supress ARP:	Enabled

# 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

Managed Network > shegde > boc Pending Changes

Mobility Master

- SC-VRRP-STBY-SHEGDE
- SC\_VM\_10.16.12.22

Managed Network (7)

- abhi (1)
- shegde (6)
  - boc (5)**
    - 7005
    - aa:bb:cc:aa:bb:cc
    - grappa (1)
    - shegde\_MN\_70
    - ouzo (1)
    - Aruba7005
    - ouzoplus (1)
    - Aruba7008
    - vpnc (1)
    - Aruba7010

Dashboard

**Configuration**

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces**
- Controllers
- System
- Tasks

Ports   VLANs   IP Routes   IPv6 Neighbors   GRE Tunnels   **Pool Management**   OSPF   Multicast

> VLAN Pools

▼ Tunnel Pools

Tunnel Pools		
NAME	START ADDRESS	END ADDRESS
abcd	33.33.33.3	33.33.33.33
abc	33.33.33.1	33.33.33.64
tunnelpool	22.22.22.0	22.22.22.19

+

**Tunnel Pool > tunnelpool**

Pool name:  Tunnel Pools

Start IP address:

End IP address:

# Tunnel Pool assignment to GRE tunnel

- Configuration -> interfaces -> GRE tunnels

The screenshot displays a network management interface for a Managed Network named 'shegde' under the 'boc' group. The interface is divided into several sections:

- Left Sidebar:** Shows a tree view of the network hierarchy. Under 'Managed Network (7)', the 'boc (5)' group is expanded, listing devices: 7005, aa:bb:cc:aa:bb:cc, grappa (1), shegde\_MN\_70, ouzo (1), Aruba7005, ouzoplus (1), Aruba7008, vpnc (1), and Aruba7010.
- Configuration Menu:** A central menu with categories: Dashboard, Configuration (highlighted), WLANs, Roles & Policies, Access Points, AP Groups, Authentication, Services, Interfaces (highlighted), Controllers, System, and Tasks.
- GRE Tunnels Tab:** The 'GRE Tunnels' tab is active, showing configuration for 'GRE Tunnel > 1'. The settings are as follows:
  - IPversion: ipv4
  - Tunnel ID: 1
  - Mode: L3 (selected)
  - IPv4 address type: Dynamic
  - Dynamic IP address pool: tunnelpool (with a red note: 'tunnel pool created under pool management tab')
  - MAC address of peer device: 00:0b:86:9a:6b:37 (with a red note: 'required to autogenerate config for peer tunnel')
  - Enable: Enabled
  - Trusted: Trusted
  - MTU: 1200
  - Tunnel source: vlan
  - Vlan: 222 (with a red note: 'must be vlan which is assigned with ip address from tunnelpool')
  - Tunnel destination: 172.66.30.1
  - Route ACL name: -None- in

# 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

Managed Network > shegde > boc Pending Changes ↻

Mobility Master

- SC-VRRP-STBY-SHEGDE
- SC\_VM\_10.16.12.22

Managed Network (7)

- abhi (1)
- shegde (6)
  - boc (5)**
    - 7005
    - aa:bb:cc:aa:bb:cc
    - grappa (1)
      - shegde\_MN\_70
    - ouzo (1)
    - Aruba7005
    - ouzoplus (1)

Dashboard

**Configuration**

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces**
- Controllers
- System
- Tasks

Ports **VLANs** IP Routes IPv6 Neighbors GRE Tunnels **Pool Management** OSPF Multicast

▼ NAT Pools

NAT Pools				
NAME	START ADDRESS	END ADDRESS	DESTINATION NAT IP	FLAGS
dynamic-srcnat	0.0.0.0	0.0.0.0	--	--
NATPOOL	10.10.10.1	10.10.10.20	20.20.20.1	Static

+

- > VLAN Pools
- > Tunnel Pools

# NAT Pool

- NAT POOL configuration in session ACL

Managed Network > shegde > boc

Mobility Master  
SC-VRRP-STBY-SHEGDE  
SC\_VM\_10.16.12.22

Managed Network (7)  
abhi (1)  
shegde (6)  
    **boc (5)**  
        7005  
        aa:bb:cc:aa:bb:cc  
        grappa (1)  
            shegde\_MN\_70  
        ouzo (1)  
            Aruba7005  
        ouzoplus (1)  
            Aruba7008  
        vpnc (1)  
            Aruba7010

Dashboard  
**Configuration**  
WLANs  
**Roles & Policies**  
Access Points  
AP Groups  
Authentication  
Services  
Interfaces  
Controllers  
System  
Tasks

Roles **Policies** Applications

+  
Roles > natpool > New forwarding Rule

IP version: IPv4  
Source: Any  
Destination: Any  
Service/app: Any  
Action: Source and Destination NAT  
NAT pool: natpool  
Port:  
TOS:  
Time range: - None - Reset  
802.1p priority:  
Options:  Log  Mirror  Blacklist  Disable Scanning

# DHCP Pool Configuration

- Configuration -> services -> dhcp server

The screenshot displays the DHCP Server configuration page. The left sidebar shows a tree view with 'Mobility Master' and 'Managed Network (7)'. Under 'Managed Network (7)', the 'boc (5)' folder is selected, containing several sub-items like '7005', 'aa:bb:cc:aa:bb:cc', 'grappa (1)', 'shegde\_MN\_70', 'ouzo (1)', 'Aruba7005', 'ouzoplus (1)', 'Aruba7008', 'vpnc (1)', and 'Aruba7010'. The main content area is divided into 'Configuration' and 'Services' sections. The 'DHCP Server' tab is active, showing various configuration fields:

Cluster	Redundancy	VPN	Firewall	IP Mobility	External Services	<b>DHCP Server</b>	WAN
IP version:		IPv4					
Pool name:		clientpool					
Default routers:							(Multiple Default Routers should be separated by spaces)
DNS servers:							(Multiple DNS Servers should be separated by spaces)
Import from DHCP/PPPoE:		<input type="checkbox"/>					
Domain name:							
WINS:							(Multiple WINS Servers should be separated by spaces)
Import from DHCP/PPPoE:		<input type="checkbox"/>					
Lease days:							
Lease hrs:							
Lease mins:							
Lease secs:							
Network IP address type:		Dynamic					
Starting network IPv4 address:		172.16.222.1					
Ending network IPv4 address:		172.16.222.254					
Hosts:		16					

# DHCP Pool Assignment

- Configuration -> interfaces -> VLAN

The screenshot displays the Aruba Mobility Master configuration interface. On the left is a navigation tree with 'Managed Network (7)' expanded to show 'shegde (6)' and 'voc (5)'. The main panel shows the 'Configuration' menu with 'Interfaces' selected. A table lists VLANs, with VLAN 222 highlighted. Below the table, the 'IP Address Assignment' settings for the selected VLAN are shown, including DHCP Pool, DHCP pool, Option-82, MTU, and Suppress ARP.

Ports	VLANs	IP Routes	IPv6 Neighbors	GRE Tunnels	Pool Management	OSPF	Multicast	
111	--	--	--	0/0/2	Enabled	N/A	Disabled	None
222	--	--	--	0/0/1	Enabled	N/A	Disabled	None
1111	--	--	--	--	--	Disabled	None	

**Port Members** | **IPv4** | **IPv6** | **More**

**IP Address Assignment**

*IP assignment:* DHCP Pool

*DHCP pool:* clientpool

*Option-82:* MAC

*MTU:* 1500

*Suppress ARP:* Enabled

> IGMP

> Other Option

Cancel Submit

ArubaMM, 8.0.0.0-svcs-ctrl

# 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

The screenshot displays the configuration page for WAN health checks in a network management system. The interface includes a sidebar with navigation options, a top navigation bar, and a main configuration area.

**Managed Network** Pending Changes

**Managed Network (1)**  
aa:bb:cc:aa:bb:cc

**Configuration**

- Dashboard
- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services**
- Interfaces
- Controllers
- System
- Tasks

**Cluster** **Redundancy** **VPN** **Firewall** **IP Mobility** **External Services** **DHCP Server** **WAN**

**Health Check**

Health check:

Remote host IP/FQDN:

**WAN**

Probe mode:  ▼

Probe interval:  Sec

Packet burst per probe:

Probe retries:

**PBR**

Probe mode:  ▼

Probe interval:  Sec

Packet burst per probe:

Probe retries:

[> WAN Optimization](#)

[> WAN Scheduler](#)

# Configuring WAN uplinks

- Configuration -> services -> WAN -> uplink

Managed Network > shegde > boc > grappa > shegde\_MN\_7010 Pending Changes

Mobility Master  
SC-VRRP-STBY-SHEGDE  
SC\_VM\_10.16.12.22

Managed Network (7)  
abhi (1)  
shegde (6)  
boc (5)  
7005  
aa:bb:cc:aa:bb:cc  
grappa (1)  
**shegde\_MN\_70**  
ouzo (1)  
Aruba7005  
ouzoplus (1)  
Aruba7008

Dashboard  
**Configuration**  
WLANs  
Roles & Policies  
Access Points  
AP Groups  
Authentication  
**Services**  
Interfaces  
Controllers  
System  
Tasks

Cluster Redundancy VPN Firewall IP Mobility External Services DHCP Server **WAN**

> WAN Optimization  
> WAN Scheduler  
▼ Uplink  
Enable uplink:   
Default wired priority:   
Default cellular priority:   
Load balancing:

**Uplink VLANs**

LINK	ID	DESCRIPTION	OPERATION STATE	PRIORITY	WEIGHT
link2	4093	uplink4093	✓	150	--
link1	4094	priuplink4094	✓	200	1

# Checking WAN uplink status

```
(host) #show uplink
```

```
Uplink Manager: Disabled
```

```
Uplink Health-check: Enabled
```

```
Uplink Health-check IP/FQDN: 192.0.2.14
```

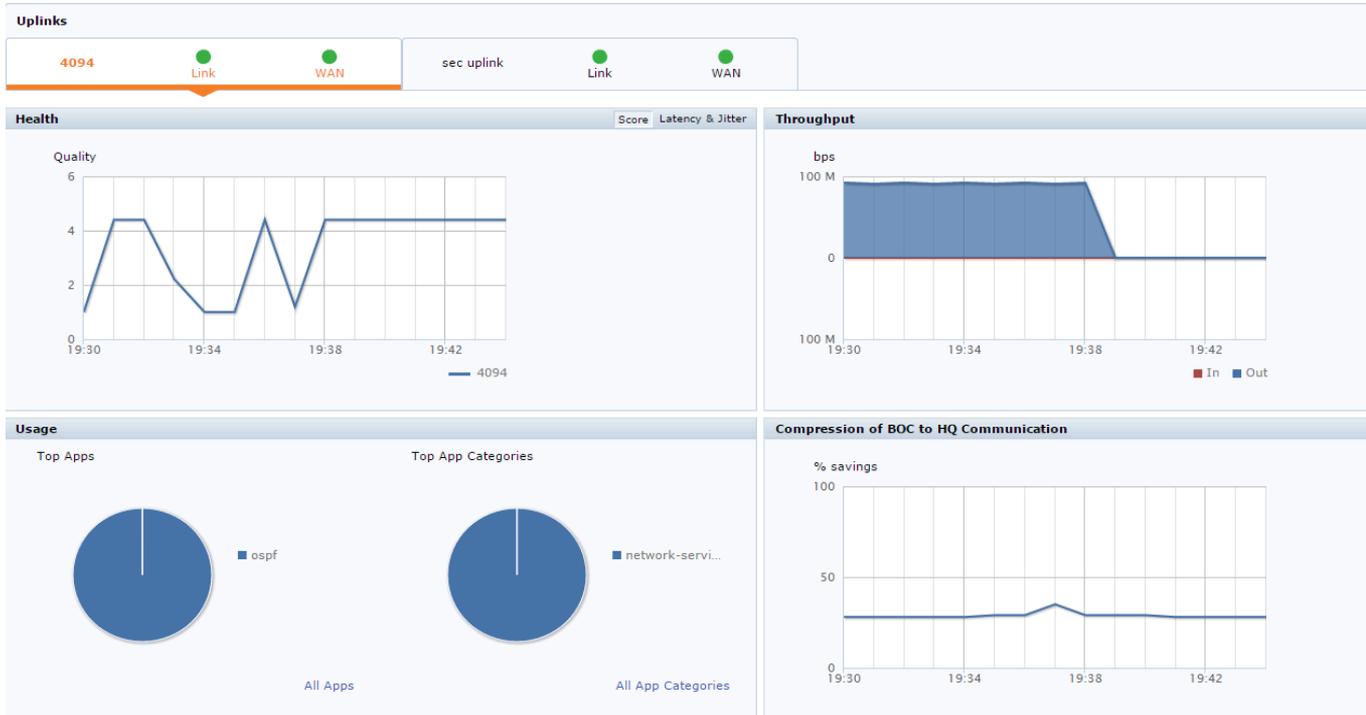
```
Uplink Management Table
```

```
-----  
Id  Uplink Type  Properties      Priority  State      Status      Reachability  
--  -
```

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