



# WiNG 5.X How-To Guide

## NOC Deployments

March 2012

Revision 2.1

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

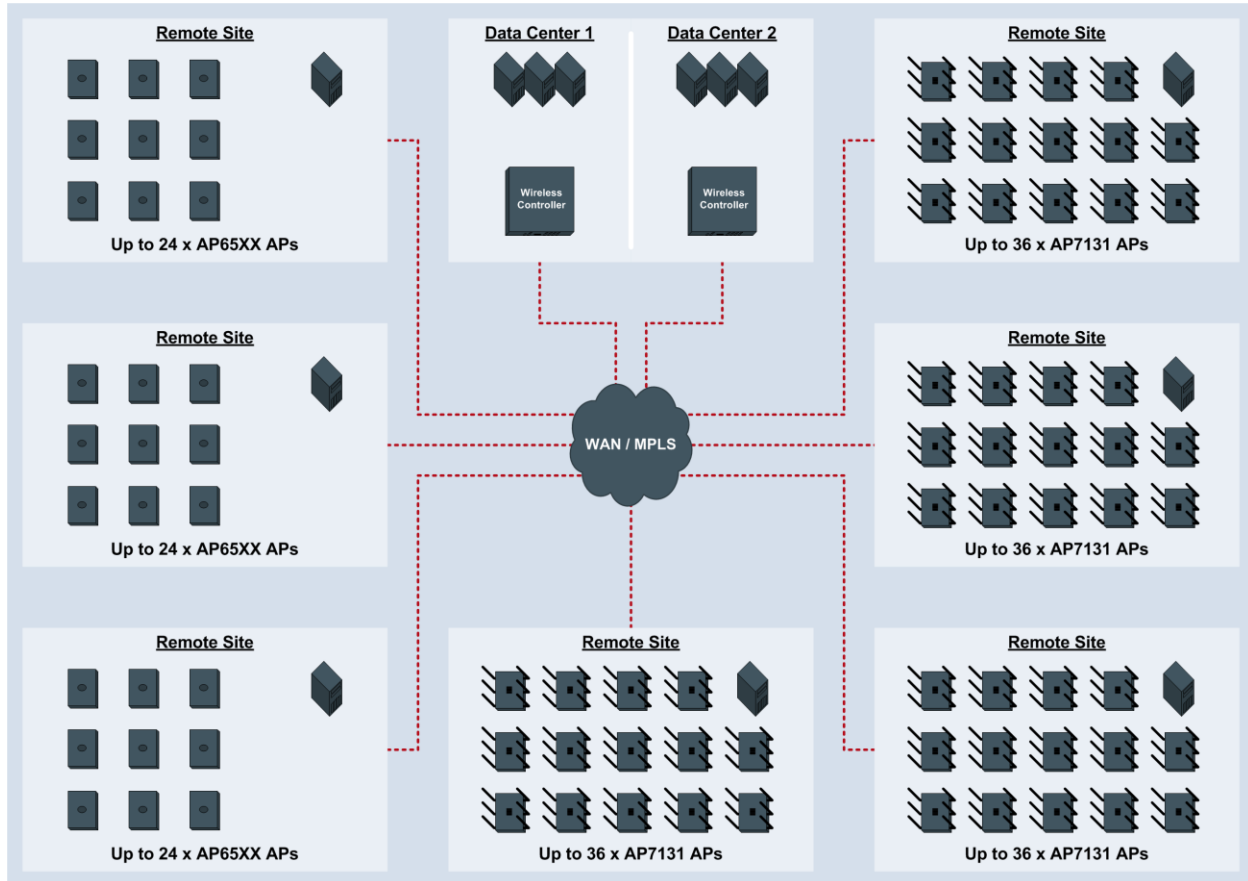
© 2012 Motorola Solutions, Inc. All Rights Reserved.

# Table of Contents

|   |    |
|---|----|
| Table of Contents.....                    | 3  |
| 1. Introduction.....                      | 4  |
| 1.1 Architecture.....                     | 5  |
| 1.2 Forwarding.....                       | 8  |
| 1.3 RADIUS Redundancy .....               | 9  |
| 1.4 Pre-Staging.....                      | 11 |
| 2. Configuration .....                    | 12 |
| 2.1 RF Domains.....                       | 14 |
| 2.2 Management Policies.....              | 20 |
| 2.3 Wireless LANs .....                   | 28 |
| 2.4 Profiles.....                         | 38 |
| 2.5 Overrides .....                       | 53 |
| 2.6 Automatic Provisioning Policies ..... | 65 |
| 2.7 Forming the Cluster .....             | 72 |
| 2.8 DHCP Services.....                    | 74 |
| 2.9 Pre-Staging Access Points.....        | 85 |
| 3. Verification.....                      | 87 |
| 3.1 Verifying Adoption Status.....        | 87 |
| 3.2 Verifying RF Domains .....            | 88 |
| 3.3 Verifying MINT .....                  | 89 |
| 4. Appendix.....                          | 91 |
| 4.1 Scaling.....                          | 91 |
| 4.2 Bandwidth Requirements .....          | 95 |
| 4.3 WiNG 5.X Protocols & Ports .....      | 97 |
| 4.4 Running Configuration .....           | 98 |

# 1. Introduction

Motorola Solutions NOC deployment model provides a highly scalable centrally managed Wireless LAN solution that is intended for customers deploying 802.11n Wireless LAN services at remote branch sites. The NOC model differs from a typical campus deployment as all the configuration and management is performed centrally on Wireless Controllers located in a data center / NOC rather than Wireless Controllers deployed locally at each site. All Wireless user traffic is bridged locally within the remote site eliminating unnecessary overhead on the WAN and potential Wireless Controller bottlenecks.



**Figure 1.0 – NOC Model**

The NOC model can be scaled to support up to 4,096 remote sites and each remote site can support up to 24 x AP65xx series or 36 x AP71X1 series Independent Access Points. AP6xx series Dependent Access Points maybe deployed, however as these Access Points are dependent on the Wireless Controllers in the NOC no survivability is provided in the event of a WAN outage or Wireless Controller failure.

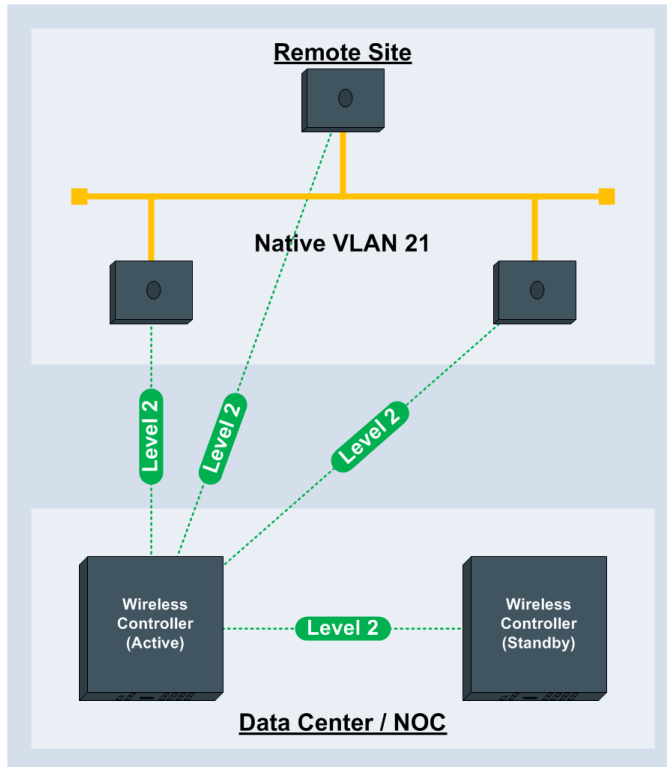
Access Points at each remote site communicate with the Wireless Controllers in the data center / NOC over a private WAN or MPLS service. To further optimize WAN bandwidth one elected Access Point at each site (the RF Domain Manager) maintains communications with the centralized Wireless Controllers. The RF Domain Manager is responsible for distributing firmware images, aggregating statistics and performing SMART RF calculations for the site.

Availability is also provided with the NOC solution at a number of different levels. AP65xx or AP71xx series Independent Access Points can be deployed to provide full site survivability in the event of a WAN outage. Each independent Access Point is fully capable of providing AAA, DHCP, Firewall, WIPS and WIDS services for the site. Unlike competing Wireless LAN solutions a WAN outage will not restrict the Wireless services or security capabilities of the remote site.

## 1.1 Architecture

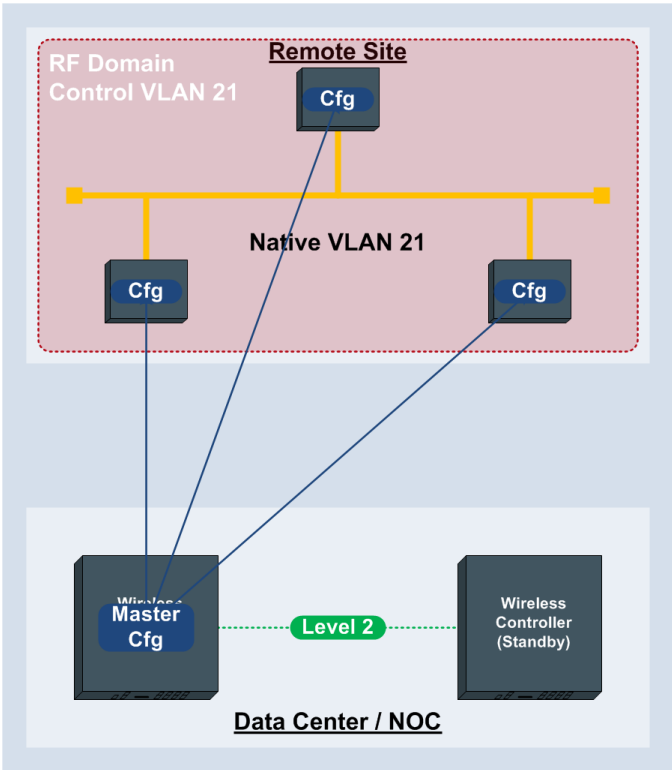
The Motorola Solutions NOC deployment model utilizes a cluster of Wireless Controllers in the data center / NOC. The cluster is configured using Level 2 IP or VLAN based MINT links rather than Level 1 MINT links typically utilized for campus deployments. Level 2 MINT links are utilized for these large scale NOC deployments so that the Access Points at each remote site are isolated from Access Points at other sites reducing the MINT routing table size on the Access Points. If Level 1 MINT links were utilized, Access Points at each site would have full visibility to all the remote Access Points in the network.

The following describes how the Access Points boot and communicate with the NOC model:



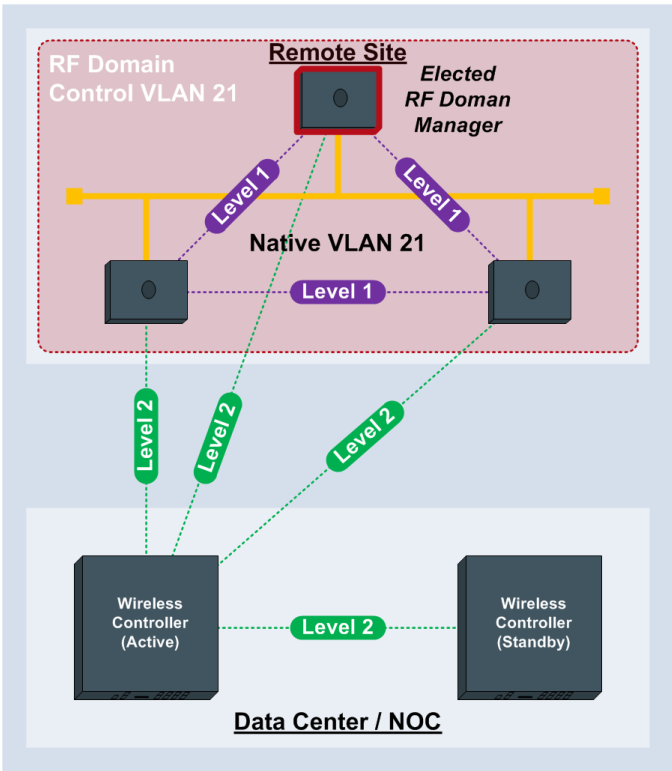
- 1) The Wireless Access Points at each remote site automatically discover the Wireless Controllers in the data center / NOC using DHCP option 191 or manually using static Controller IP addresses / Hostnames defined during staging.

During initialization the remote Access Points use DHCP option 191 or static configuration to establish a Level 2 IP based MINT link to a Wireless Controller in the data center / NOC. The Access Point is either load-balanced to the least loaded Wireless Controller in the cluster based on load or is steered to a specific Wireless Controller using the Preferred Controller Group name.

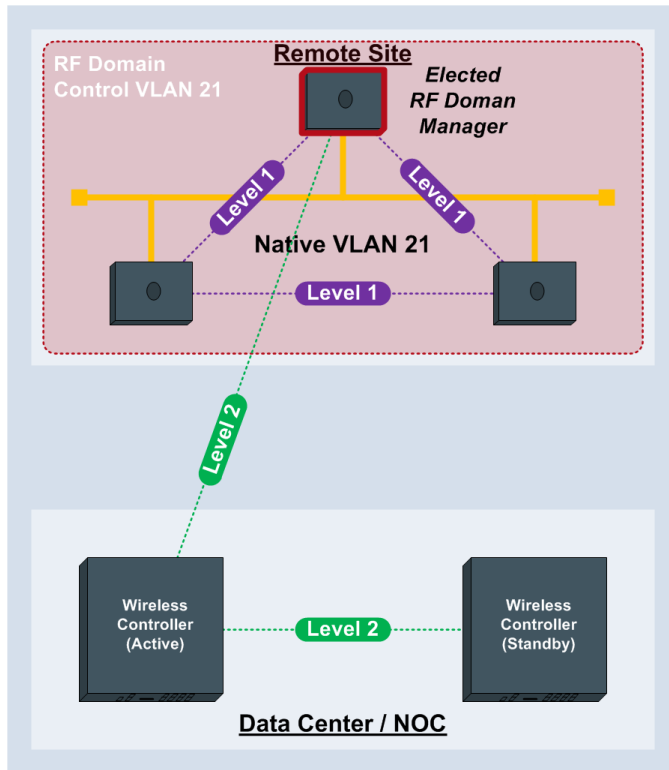


2) Once a Level 2 IP based MINT link to a Wireless Controller has been established, the Access Points receive their configuration which includes its assigned RF Domain and Profile in addition to any Device overrides, Wireless LANs and Policies.

Each remote site is assigned a unique to a unique RF Domain which includes a Control VLAN definition for the remote site. The Control VLAN is typically the Native VLAN that all the Access Points at the remote site are connected to.



3) The Access Points at the remote site use their Control VLAN to establish a Level 1 VLAN based MINT link to discover all the neighboring Access Points at the site. The Access Points then elect one of the Access Points as the RF Domain Manager for the site which is responsible for firmware updated, statistic collection and SMART RF calculations.



- 4) All the Access Points except the elected RF Domain Manager tear down their Level 2 IP based MINT links to their Wireless Controller at the data center / NOC. If the elected RF Domain Manager fails, another Access Point will be automatically elected.

**Figure 1.1 – NOC Architecture**

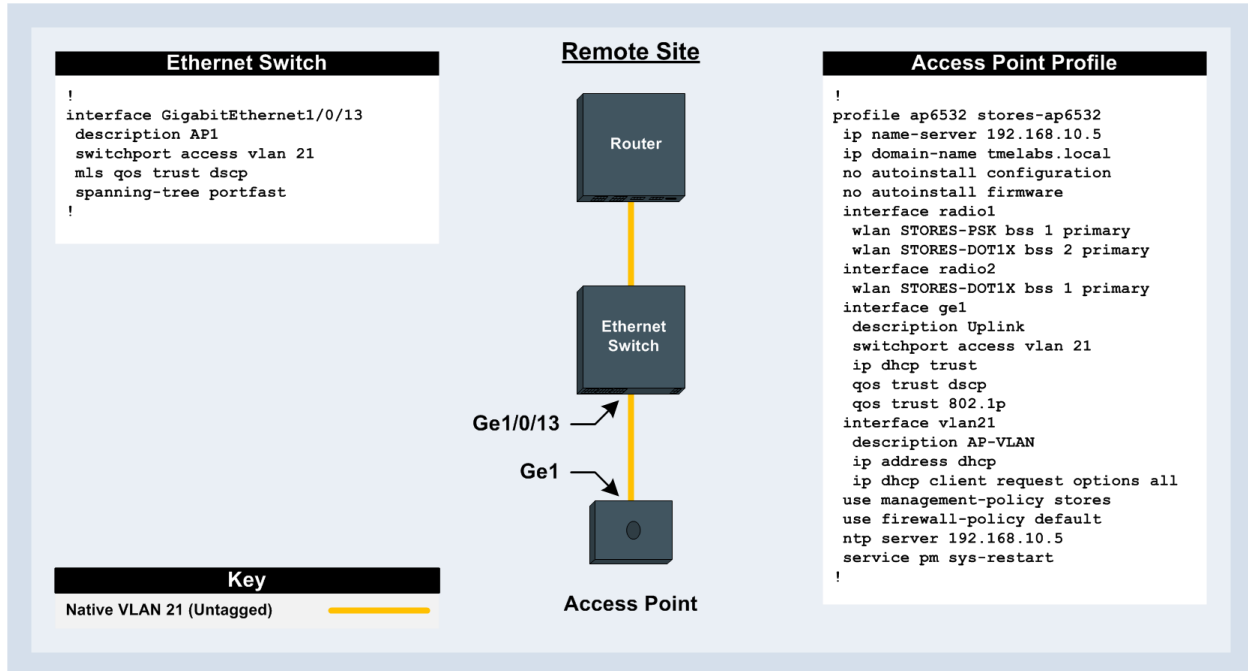
Once the Access Points at the remote site are operational, MINT communications between the data center / NOC and remote Access Points occurs through the elected RF Domain Manager for the site. The remote Access Points are managed as if they were connected to the Wireless Controllers over Level 1 MINT links.



Note – As Level 2 IP based MINT links are used between the remote sites and the data center / NOC, Extended VLANs are not supported. No Wireless User traffic can be tunneled from the Access Points to the centralized Wireless Controllers using this deployment model.

## 1.2 Forwarding

Access Points deployed at remote sites forward traffic locally within the site and no traffic can be tunneled to the Wireless Controllers in the data center / NOC. If the wireless user traffic at the remote site is mapped to a single VLAN, a single untagged Native VLAN can be deployed at the site and 802.1Q tagging does not need to be enabled. If a Native VLAN id other than 1 is deployed at the remote site, it is strongly recommended that the Native VLAN id match between the Ethernet switch ports and the GE1 ports on the Access Points.



**Figure 1.2.1 – Single Untagged Native VLAN**

If wireless users are mapped to multiple different VLANs at the site, 802.1Q VLAN tagging must be enabled on both the Access Points Ge1 ports as well as the Ethernet switch ports the Access Points are connected to. The Native VLAN id and Allowed VLANs on both the Ethernet switch ports and the Access Points Ge1 ports must match or wireless user traffic maybe be dropped.

For plug-n-play Access Point deployments it recommended that the Access Points Native VLAN id at each remote site be configured as untagged. New Access Points deployed at a site will automatically obtain network addressing over their default VLAN 1. If the Ethernet switch port is configured to tag the Native VLAN and drop untagged frames, new Access Points will be unable to communicate with the network and discover the Wireless Controllers in the data center / NOC to receive their configuration.

Configuring the Native VLAN as untagged permits Controller discovery and will allow a new Access Point to adopt and receive its configuration. A new Access Point will obtain network addressing over VLAN 1, discover the Wireless Controllers in the data center / NOC using DHCP option 191, adopt and receive their configuration which includes the new Native VLAN id. Once received the Access Point will switch to the new Native VLAN id and obtain network addressing using the new Virtual IP interface and re-establish communications with the Wireless Controllers in the data center / NOC.



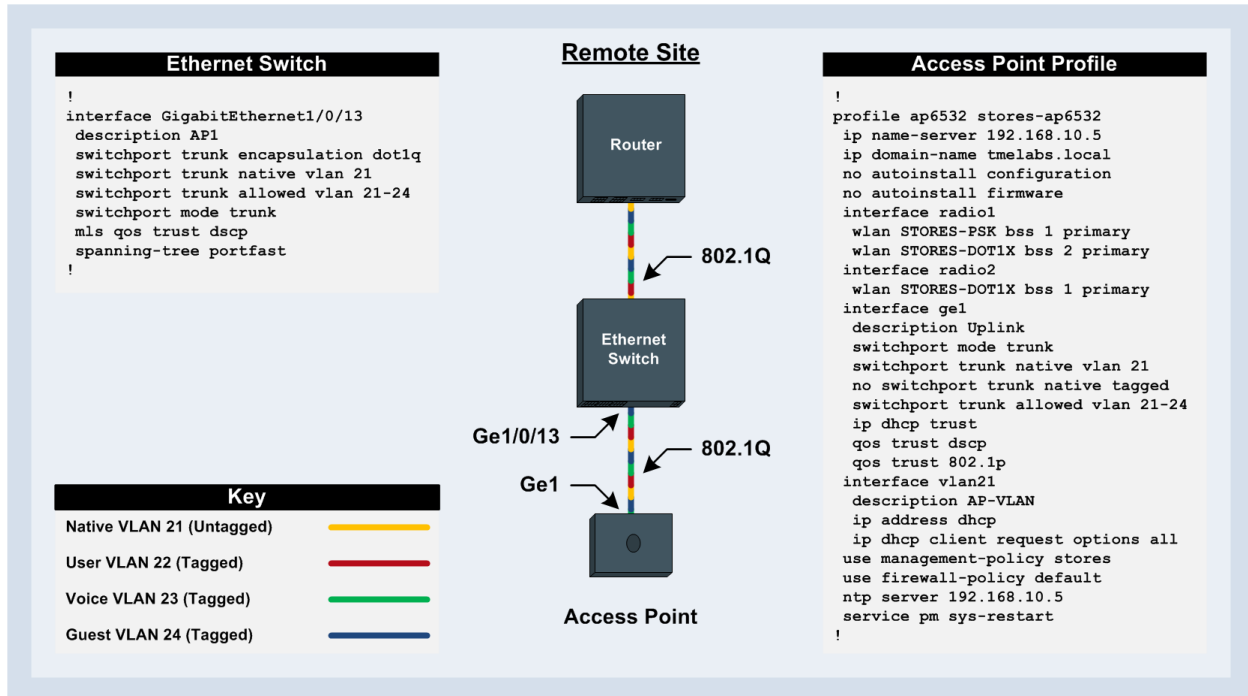


Figure 1.2.2 – 802.1Q Tagged Deployment

## 1.3 RADIUS Redundancy

For remote Access Point deployments RADIUS AAA services are typically provided centrally within the data center / NOC where multiple redundant RADIUS AAA servers are deployed. However RADIUS AAA servers may also be deployed locally at each remote site using physical servers or on network infrastructure such as Routers or a WiNG 5.X device.

The RADIUS AAA servers used to authenticate wireless users is defined in AAA Policies which are assigned to individual Wireless LANs or Hotspot Policies. Each AAA Policy can include up to six RADIUS Authentication and Accounting server entries which can be load-balanced (round-robin) or provide fail-over. Each Authentication or Accounting server entry supports three different Server Types:

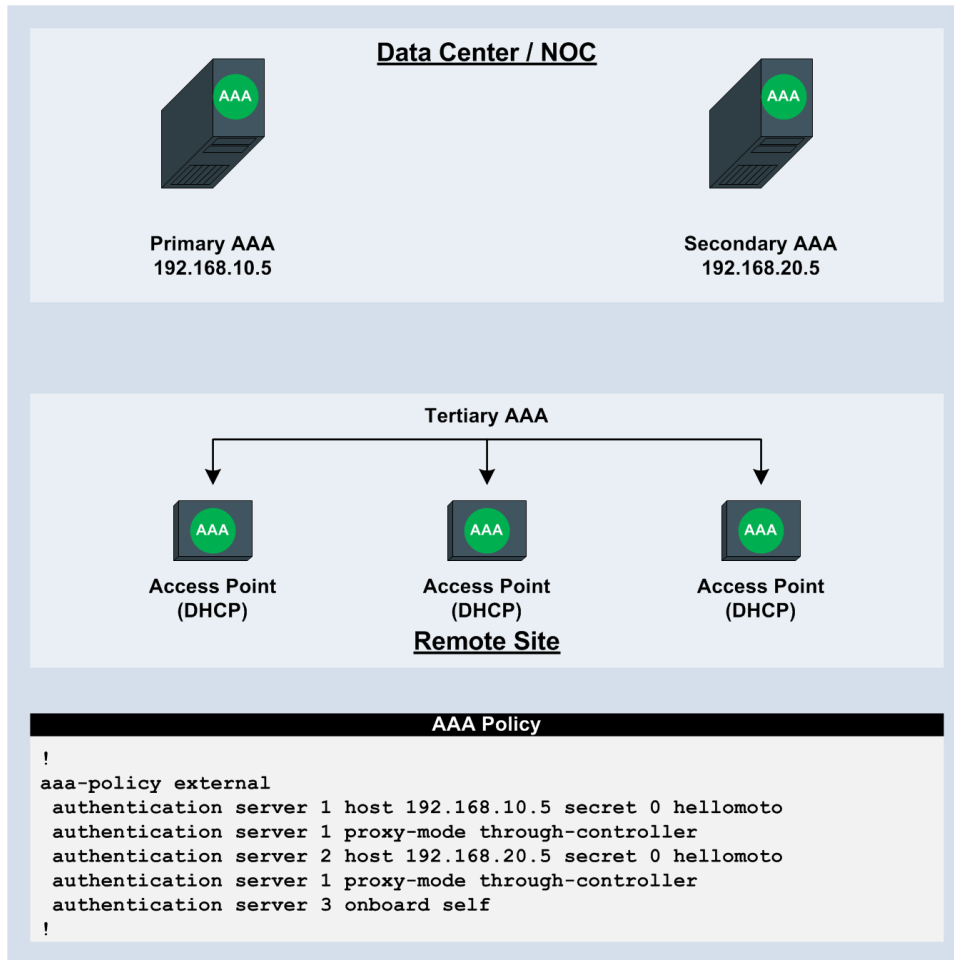
- Host – RADIUS server is hosted on an external host.
- Onboard Self – RADIUS server is hosted locally on the Access Point.
- Onboard Controller – RADIUS server is hosted on the Wireless Controller managing the Access Point.

For each Server Type WiNG 5.X also supports a Proxy Request Mode which determines how RADIUS Authentication and Accounting requests are forwarded. RADIUS Authentication and Accounting requests can be forwarded directly from the Access Points to the RADIUS server, proxied through the elected RF Domain Manager at the remote site or be forwarded through the Wireless Controllers in the data center / NOC.

If no RADIUS servers are available at a remote site, existing authenticated users will continue to operate with no interruption as by default user credentials are cached by the Access Points for up to 24 hours. However new users connected to Wireless LANs that require authentication will require an available RADIUS server before being permitted access to the network.

RADIUS Authentication redundancy can be provided in a number of different ways. During normal operation RADIUS Authentication and Accounting requests can be forwarded to a primary RADIUS server in the data center NOC which is backed up by a second RADIUS server either located in the same

data center or an alternate data center. If data center communications are disrupted, RADIUS Authentication can be provided locally at the remote site either using a locally deployed RADIUS server, RADIUS service running on a Router or locally on each Independent Access Point.



**Figure 1.3 – AAA Redundancy Example**

When backup RADIUS services are provided locally on the Independent Access Points at a site, a RADIUS Server Policy will need to be defined and assigned to the Access Point Profile. The RADIUS Server Policy includes the RADIUS Server configuration along with specific User Pools. During a WAN outage, each Independent Access Point will be fully capable of authenticating EAP or Hotspot users locally providing no interruption to Wireless services at the remote site.

## 1.4 Pre-Staging

Remote Access Points can automatically or manually discover Wireless Controllers in the data center / NOC. Automatic discovery can be provided using DHCP option 191 while manual configuration can be performed by statically defining controller IP addresses or hostnames to each remote Access Point. Most NOC deployments will utilize automatic discovery using DHCP option 191 as it permits zero-touch Access Point deployments.

Manual Wireless Controller discovery requires certain parameters to be pre-configured on an Independent Access Point before it can be adopted for the first time (i.e. pre-staging). For example a Native VLAN id, Virtual IP Interface, Default Route and Controller IP Address / Hostname would all need to be pre-defined before an Independent Access Point is able to communicate over the network and discover the Wireless Controllers in the data center / NOC.

When an Access Point is adopted by a Wireless Controller in the data center / NOC, the cluster master pushes configuration to the joining Access Point. The configuration could potentially be different from the pre-staged configuration of the device. Specifically VLAN and IP addressing parameters could be different preventing any further communications with the remote Access Point.

To address this challenge WiNG 5.X provides the ability to preserve certain relevant parts of an Independent Access Points pre-staged configuration as the Access Points is adopted. During initial adoption the newly discovered Access Point forwards specific pre-defined configuration parameters from its configuration to the Wireless Controller. These configuration parameters are then applied to the Access Points Device configuration as Overrides along with a Profile and RF Domain assignment as the device is added to the system.

The following provides a list of configuration parameters which are maintained during initial adoption:

- Static Routes
- Name Server
- Domain Name
- Hostname
- Controller Hosts
- Interface Speed
- Interface Duplex
- Native VLANs
- Tagged VLANs
- Virtual IP Interfaces

Pre-staging only functions for Access Points that have not been previously discovered by the Wireless Controllers in the data center / NOC. The Wireless Controllers will ignore any pre-staged configuration from Access Points that are already present in the configuration.

## 2. Configuration

This section provides the necessary configuration steps required to provision a cluster of Wireless Controllers in a data center / NOC to support remote AP6532 Access Point deployments. In the following configuration example two RFS6000 Wireless Controllers will be configured in the data center NOC as an Active / Active cluster supporting two remote sites (Store 100 and Store 101). As the VLANs are common within the data center / NOC and each remote site, one user defined Profile will be required for the Wireless Controllers and the remote Access Points:

- One user defined RF Domain will be defined for the NOC and each remote site.
- Separate user defined Management Policies will be defined and assigned to the Wireless Controllers in the data center / NOC and remote Access Points.
- Common configuration parameters and policies will be assigned to the RFS6000 Wireless Controllers in the data center / NOC and the AP6532 remote Access Points using user defined Profiles.
- Two 802.11i Wireless LANs will be defined and assigned to AP6532 Access Point radios using the AP6532 user defined Profile.
- Static IP addressing and cluster configuration will be assigned to each of the RFS6000 Wireless Controllers as Device overrides.
- An Automatic Provisioning Policy will be defined and assigned to the RFS6000 user defined profile.

Configuration examples will be provided for both CLI and the HTTP User Management Interface.

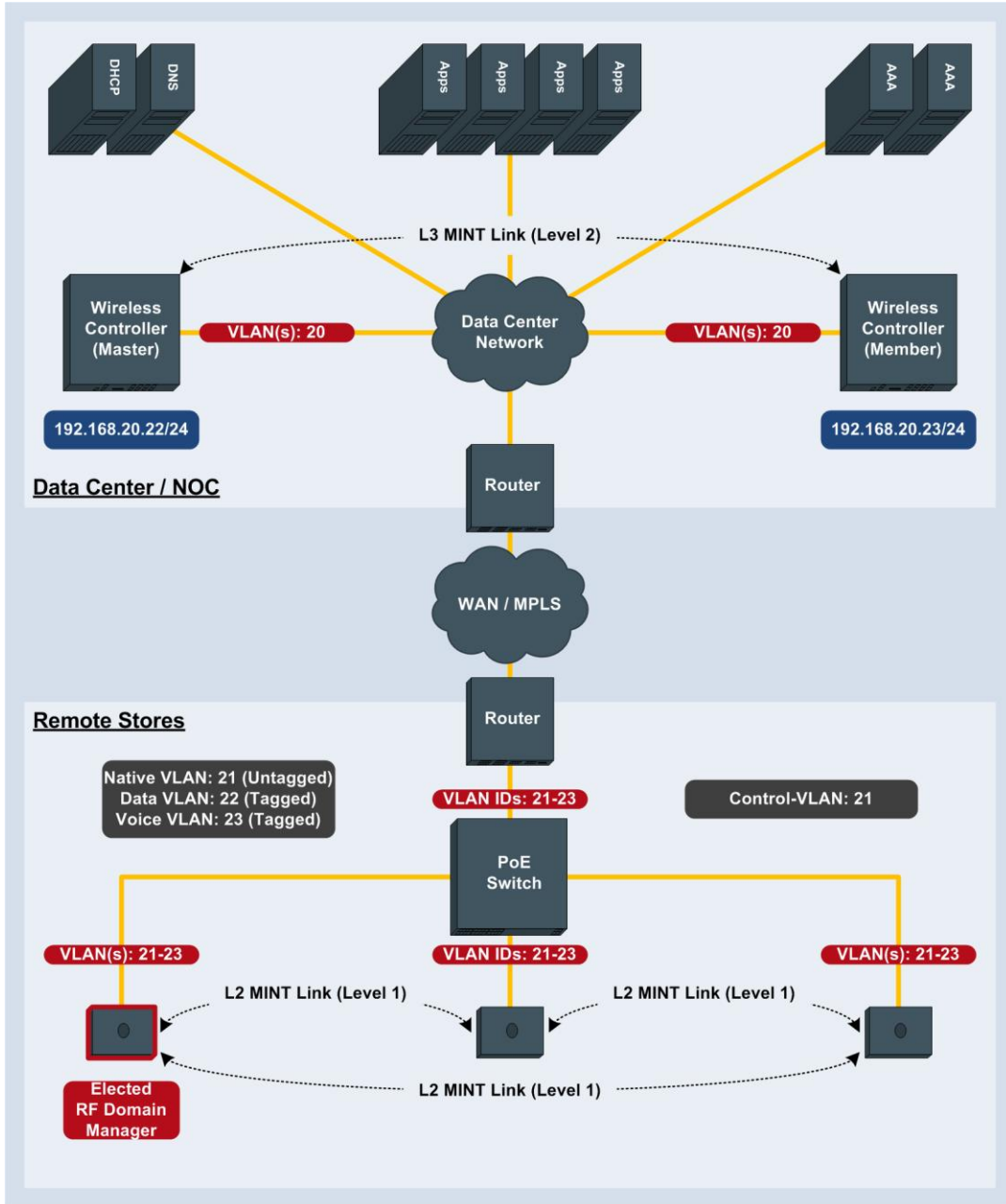


Figure 2.1 – Data Center / NOC Topology



Note – For this configuration example two RFS6000 series Wireless Controllers and AP6532 Access Points are used. It's important to note that these configuration steps are applicable to the RFS7000 and NX9000 series Wireless Controllers as well as other Motorola Access Points.



Note – Please reference the Install Guide for your Wireless Controller for the correct procedure to initially connect to the CLI or Management User Interface.

## 2.1 RF Domains

RF Domains allow administrators to assign regional and regulatory, RF and WIPS configuration to devices deployed in a common coverage area such as a remote branch site. Each RF Domain contains mandatory regulatory configuration parameters and optional contact, WIPS and SMART RF configuration.

RF Domains also provide the ability to allow administrators to override Wireless LAN SSID names and VLAN assignments for Access Points assigned to the RF Domain. This allows enterprises to deploy common Wireless LANs across multiple sites while permitting unique SSID names or VLAN assignments for each site.

One RF Domain can be assigned per Wireless Controller and Access Point and by default all devices are assigned to an RF Domain named default. For this configuration example the Wireless Controllers in the data center / NOC and the Access Points at each remote site will be assigned to a unique user defined RF Domain. Each user defined RF Domain will define regional and regulatory information as well as location and contact information.

In addition the RF Domains for each remote site will include a Control VLAN parameter which will allow the remote Access Points at each site to discover themselves over their Native VLAN and form Level 1 VLAN based MINT links between themselves. The Control VLAN is necessary so that an RF Domain manager can be elected for each site. The RF Domain manager is responsible for aggregating statistics, performing SMART RF calculations and may distribute firmware images for the site. The RF Domain Manager for each remote site is automatically elected, however you can optionally determine which Access Point will become the RF Domain Manager for a site by assigning an RF Domain Manager priority value of 255 as an Override to a specific Access Point.

For this configuration step three user defined RF Domains will be created with the following parameters:

- 1) A user defined RF Domain named ***noc*** will be created for the Wireless Controllers in the data center / NOC with the following parameters:
  - a. The ***Country Code*** will be set to ***US***
  - b. The ***Location*** will be set to ***SanJoseCA***
  - c. The ***Time Zone*** will be set to ***PST8PDT***
  - d. The ***Contact*** will be set to ***admin@tmelabs.local***.
- 2) A user defined RF Domain named ***store100*** will be created for the Access Points in store 100 with the following parameters:
  - a. The ***Country Code*** will be set to ***US***
  - b. The ***Location*** will be set to ***SanJoseCA***
  - c. The ***Time Zone*** will be set to ***PST8PDT***
  - d. The ***Contact*** will be set to ***admin@tmelabs.local***.
  - e. The ***Control VLAN*** will be set to ***21***.
- 3) A user defined RF Domain named ***store101*** will be created for the Access Points in store 101 with the following parameters:
  - a. The ***Country Code*** will be set to ***US***
  - b. The ***Location*** will be set to ***PleasantonCA***
  - c. The ***Time Zone*** will be set to ***PST8PDT***
  - d. The ***Contact*** will be set to ***admin@tmelabs.local***.
  - e. The ***Control VLAN*** will be set to ***21***.

The user defined RF Domain named **noc** will be manually assigned to each Wireless Controller in the data center using Device configuration. The RF Domains named **store100** and **store101** will be automatically assigned to Access Points deployed in both sites using Automatic Provisioning Policies.



Note – One unique RF Domain is required per remote site.



Note – The Control VLAN ID must be set to a VLAN ID that is common between all the Access Points at the remote site. In most cases this will be the untagged Native VLAN id the Access Points use to communicate with the Wireless Controllers in the data center / NOC.



Note – You can pre-select a specific Access Point as RF Domain Manager for a site by issuing the **rf-domain-manager priority** command as a device Override and assigning a priority value of **255**.

## 2.1.1 Command Line Interface

Use the following procedure to create a user defined RF Domains for the Wireless Controllers in the data center / NOC and the remote Access Points for each store using the Command Line Interface:

### 1 Create the user defined RF Domain for the Wireless Controllers in the data center named **noc** and define **Country Code**, **Location**, **Time Zone** and **Contact** parameters:

```
rfs6000-64435A(config)# rf-domain noc

rfs6000-64435A(config-rf-domain-noc)# country-code us

rfs6000-64435A(config-rf-domain-noc)# location SanJoseCA

rfs6000-64435A(config-rf-domain-noc)# timezone PST8PDT

rfs6000-64435A(config-rf-domain-noc)# contact admin@tmelabs.local
```

### 2 Verify the changes:

```
rfs6000-64435A(config-rf-domain-noc)# show context

rf-domain noc
location SanJoseCA
contact admin@tmelabs.local
timezone PST8PDT
country-code us
```

### 3 Exit the RF Domain configuration:

```
rfs6000-64435A(config-rf-domain-noc)# exit
```

#### 4 Create the user defined RF Domain for the Access Points in store 100 named *store100* and define *Country Code*, *Location*, *Time Zone* and *Contact* parameters:

```
rfs6000-64435A(config)# rf-domain store100

rfs6000-64435A(config-rf-domain-store100)# country-code us
rfs6000-64435A(config-rf-domain-store100)# location SanJoseCA
rfs6000-64435A(config-rf-domain-store100)# timezone PST8PDT
rfs6000-64435A(config-rf-domain-store100)# contact admin@tmelabs.local
rfs6000-64435A(config-rf-domain-store100)# control-vlan 21
```

#### 5 Verify the changes:

```
rfs6000-64435A(config-rf-domain-store100)# show context

rf-domain store100
  location SanJoeCA
  contact admin@tmelabs.local
  timezone PST8PDT
  country-code us
  control-vlan 21
```

#### 6 Exit the RF Domain configuration:

```
rfs6000-64435A(config-rf-domain-store100)# exit
```

#### 7 Create the user defined RF Domain for the Access Points in store 101 named *store101* and define *Country Code*, *Location*, *Time Zone* and *Contact* parameters:

```
rfs6000-64435A(config)# rf-domain store101

rfs6000-64435A(config-rf-domain-store101)# country-code us
rfs6000-64435A(config-rf-domain-store101)# location PleasontonCA
rfs6000-64435A(config-rf-domain-store101)# timezone PST8PDT
rfs6000-64435A(config-rf-domain-store101)# contact admin@tmelabs.local
rfs6000-64435A(config-rf-domain-store101)# control-vlan 21
```

#### 8 Verify the changes:

```
rfs6000-64435A(config-rf-domain-store101)# show context

rf-domain store101
  location PleasontonCA
  contact admin@tmelabs.local
  timezone PST8PDT
  country-code us
  control-vlan 21
```



**9 Exit the RF Domain configuration then *commit* and *save* the changes:**

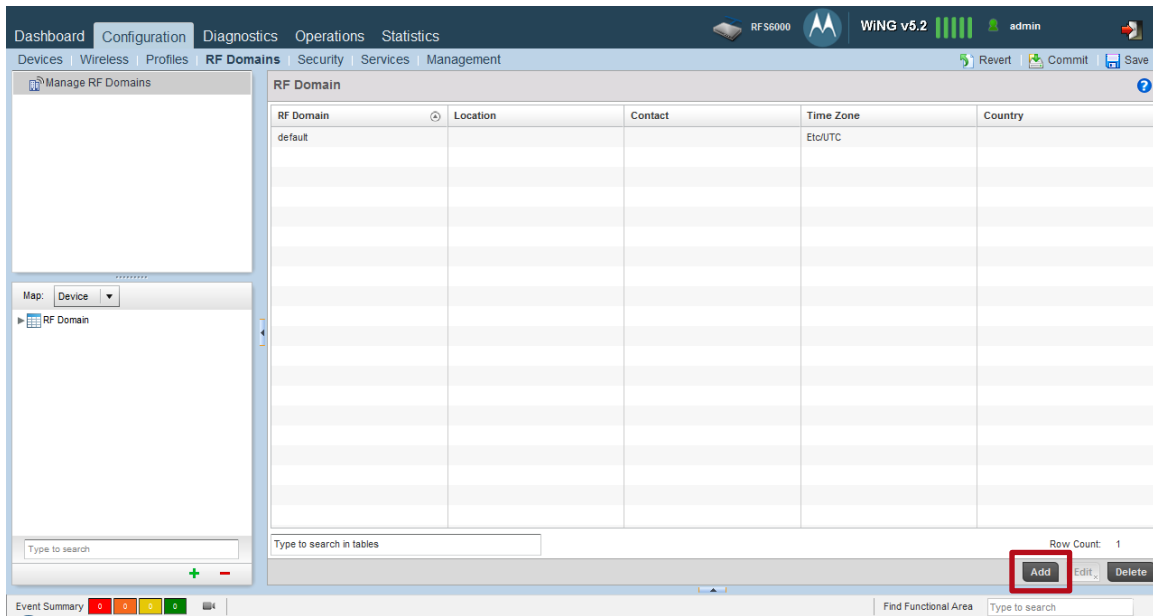
```
rfs6000-64435A(config-rf-domain-store101)# exit
rfs6000-64435A(config)# commit write

[OK]
```

## 2.1.2 Management User Interface

Use the following procedure to create a user defined RF Domains for the Wireless Controllers in the data center / NOC and the remote Access Points for each store using the User Management Interface:

**1 Select *Configuration* → *RF Domains* → *Add*:**



- 2 Enter the *RF Domain* name *noc* then enter the *Location* and *Contact* information. Select a *Time Zone* and *Country Code* then click *OK* and *Exit*:

The screenshot shows the 'RF Domain' configuration window for the domain 'noc'. The 'Basic Configuration' section is highlighted with a red box and contains the following fields:

- Location: SanJoseCA
- Contact: admin@tmelabs.local
- Time Zone: (GMT-08:00) PST8PDT
- Country: United States-us
- VLAN for Control Traffic: 1 (1 to 4,094)

The 'SMART RF' section is also visible, including 'SMART RF Policy', 'Enable Dynamic Channel', '2.4 GHz Channels', '5 GHz Channels', and '2.4 GHz Radios'. At the bottom right, the 'OK', 'Reset', and 'Exit' buttons are highlighted with red boxes.

- 3 Click *Add* to create an RF Domain for store 100. Enter the *RF Domain* name *store100* then enter the *Location*, *Contact* and *Control VLAN* information. Select a *Time Zone* and *Country Code* then click *OK* and *Exit*. Note in this example the Control VLAN is set to the Access Points untagged Native VLAN ID 21:

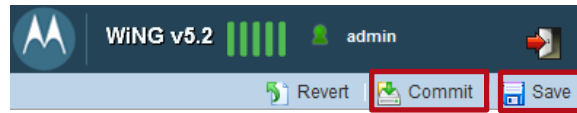
The screenshot shows the 'RF Domain' configuration window for the domain 'store100'. The 'Basic Configuration' section is highlighted with a red box and contains the following fields:

- Location: SanJoeCA
- Contact: admin@tmelabs.local
- Time Zone: (GMT-08:00) PST8PDT
- Country: United States-us
- VLAN for Control Traffic:  21 (1 to 4,094)

The 'SMART RF' section is also visible, including 'SMART RF Policy', 'Enable Dynamic Channel', '2.4 GHz Channels', '5 GHz Channels', and '2.4 GHz Radios'. At the bottom right, the 'OK', 'Reset', and 'Exit' buttons are highlighted with red boxes.



## 6 Commit then Save the changes:



## 2.2 Management Policies

Management Policies control administrative access and permissions into WiNG 5.X devices as well as control which management interfaces are enabled. Management Policies can be assigned to groups of devices using Profiles or to individual devices as Overrides.

Device administrators can be authenticated locally by the WiNG 5.X device or centrally on a RADIUS or TACACS+ server. Local authentication requires a username and password in addition to the user's role and access permissions. Remote authentication requires return attributes for the role and access permissions to be provided to the WiNG 5.X device so that the appropriate access is provided to the user.

By default all devices are automatically assigned to a Management Policy named default. For this configuration example the Wireless Controllers and remote Access Points will be assigned to different Management policies. Depending on the management strategy a single Management Policy can be utilized to manage all the Wireless Controllers or Access Points in the network or separate Management Policies can be deployed for the Wireless Controllers and Access Points. Management Policies may also be defined and assigned for Access Points at each remote site.

For this configuration step two user defined Management Policies will be created with the following parameters:

- 1) A user defined Management Policy named **noc** will be created to manage the Wireless Controllers in the data center / NOC with the following parameters:
  - a. An administrative user account **admin** with the password **hellomoto** will be created and assigned to the **Superuser** role with permissions to access **All** management interfaces.
  - b. **HTTP** will be disabled and **HTTPS** and **SSHv2** secure management interfaces will be enabled.
- 2) A user defined Management Policy named **stores** will be created to manage all the remote Access Points with the following parameters:
  - a. An administrative user account **admin** with the password **hellomoto** will be created and assigned to the **Superuser** role with permissions to access the **SSHv2** management interface.
  - b. **HTTP** will be disabled and the **SSHv2** secure management interface will be enabled.

The user defined Management Policies will be assigned to the Wireless Controllers and remote Access Points using user defined device Profiles:



Note – As AP6532 Access Points are used in this example, the serial console and HTTP management interfaces will be disabled on Management Policy assigned to the Access Points.

## 2.2.1 Command Line Interface

Use the following procedure to create a user defined Management Policies for the Wireless Controllers in the data center / NOC and the remote Access Points for each store using the Command Line Interface:

- 1 Create the user defined Management Policy for the Wireless Controllers in the data center named *noc* and define a *admin* user account and *password* with an assigned *role* and *access* permissions. In addition enable/disable *HTTP* and enable the secure *HTTPs* and *SSHv2* management interfaces:**

```
rfs6000-64435A(config)# management-policy noc

rfs6000-64435A(config-management-policy-noc)# user admin password hellomoto role
superuser access all

rfs6000-64435A(config-management-policy-noc)# no http server
rfs6000-64435A(config-management-policy-noc)# ssh
rfs6000-64435A(config-management-policy-noc)# https server
```

- 2 Verify the changes:**

```
rfs6000-64435A(config-management-policy-noc)# show context

management-policy noc
no http server
https server
ssh
user admin password 1 <encrypted-string> role superuser access all
```

- 3 Exit the Management Policy configuration:**

```
rfs6000-64435A(config-management-policy-noc)# exit
```

- 4 Create the user defined Management Policy for all the remote Access Points named *stores* and define a *admin* user account and *password* with an assigned *role* and *access* permissions. In addition disable *HTTP* and enable the secure *SSHv2* management interface:**

```
rfs6000-64435A(config)# management-policy stores

rfs6000-64435A(config-management-policy-stores)# user admin password hellomoto role
superuser access all

rfs6000-64435A(config-management-policy-stores)# no http server
rfs6000-64435A(config-management-policy-stores)# ssh
```

- 5 Verify the changes:**

```
rfs6000-64435A(config-management-policy-stores)# show context

management-policy stores
no http server
ssh
user admin password 1 <encrypted-string> role superuser access all
```

**6 Exit the Management Policy configuration then *commit* and *save* the changes:**

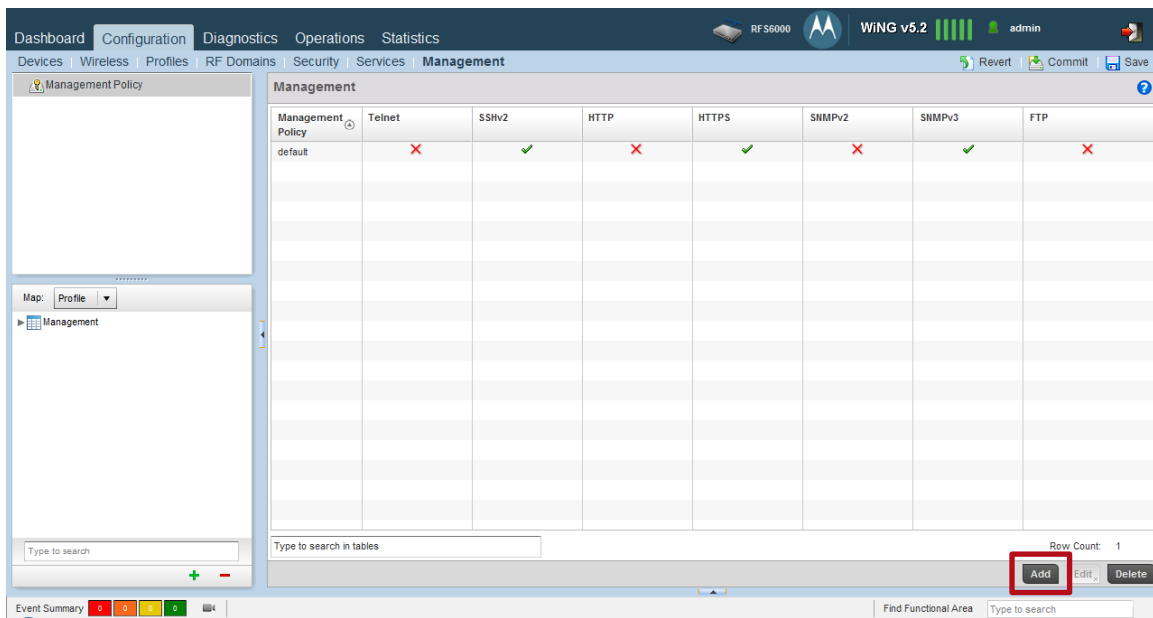
```
rfs6000-1(config-management-policy-stores)# exit
rfs6000-1(config)# commit write

[OK]
```

## 2.2.2 Management User Interface

Use the following procedure to create a user defined Management Policies for the Wireless Controllers in the data center / NOC and the remote Access Points for each store using the Management User Interface:

**1 Select *Configuration* → *Management* → *Add*:**



2 Enter the *Management Policy* name *noc* then click *Continue*:

Management Policy noc [Continue] [Exit]

Administrators Access Control Authentication SNMP SNMP Traps

| User Name | Access Type | Role |
|-----------|-------------|------|
|-----------|-------------|------|

Type to search in tables Row Count: 0

[Add] [Edit] [Delete] [Exit]

3 Select *Administrators* → *Add*:

Management Policy noc

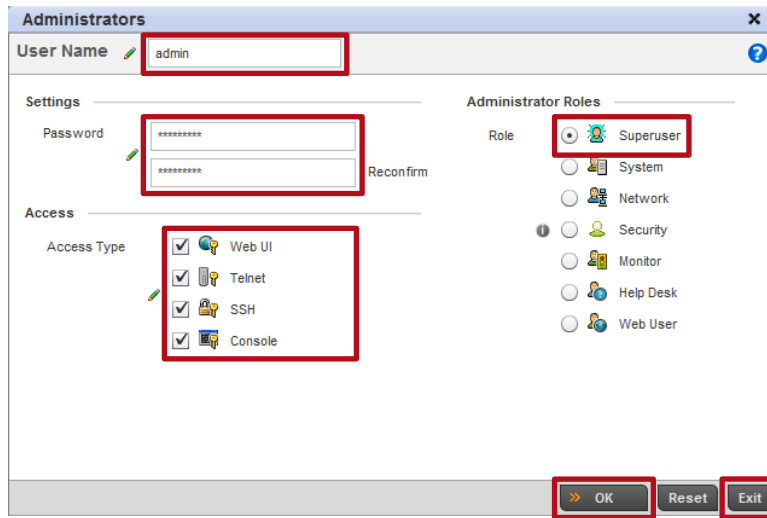
Administrators Access Control Authentication SNMP SNMP Traps

| User Name | Access Type | Role |
|-----------|-------------|------|
|-----------|-------------|------|

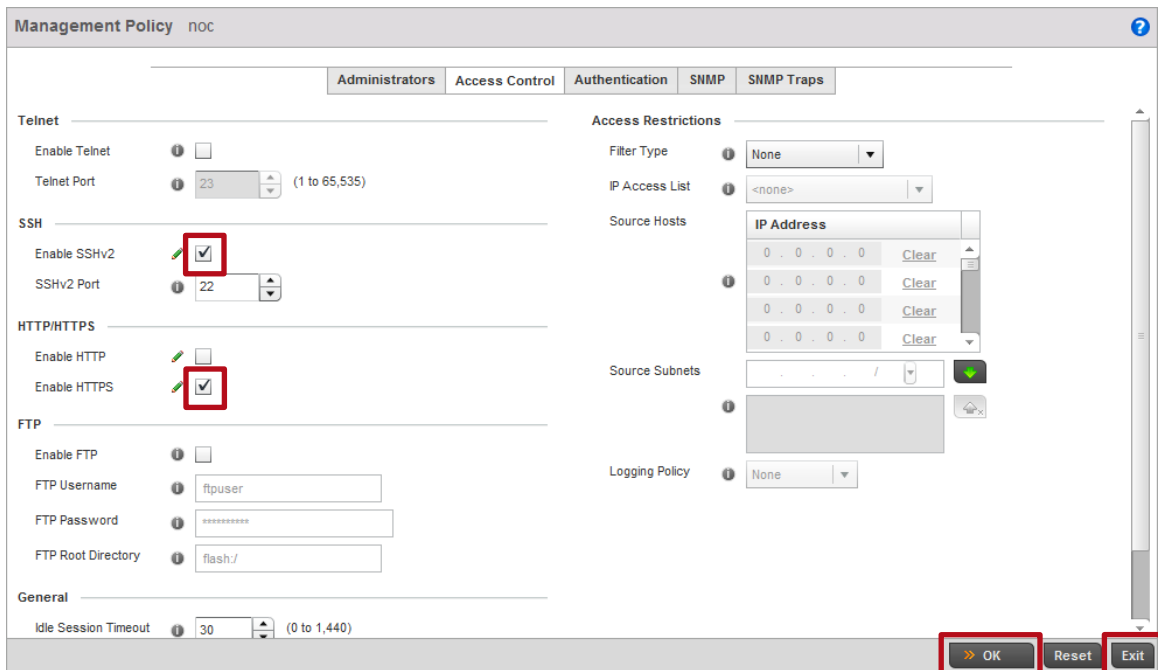
Type to search in tables Row Count: 0

[Add] [Edit] [Delete] [Exit]

- 4 Enter an admin *User Name* and *Password* then select *Role* named *Superuser*. Enable *All* the *Access Types* then click *OK* and *Exit*:



- 5 Select *Access Control* tab. Disable *HTTP* then enable the *SSHv2* and *HTTPS* secure management interfaces. Click *OK* and *Exit*:





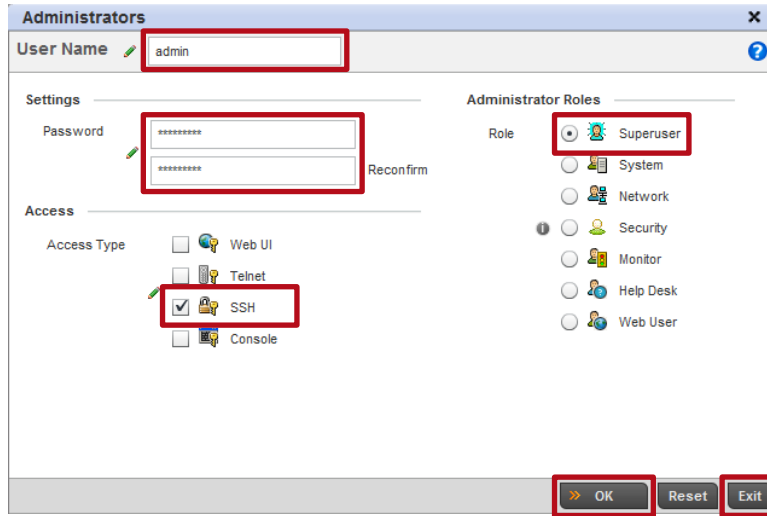
6 Click *Add* to create a user defined Management Policy for the remote Access Points. Enter the *Management Policy* name *stores* then click *Continue*:

The screenshot shows the 'Management Policy' configuration interface. At the top, there is a header bar with the text 'Management Policy' and a search icon. Below this, there is a text input field containing the name 'stores', which is highlighted with a red box. To the right of the input field are two buttons: 'Continue' and 'Exit', both also highlighted with red boxes. Below the header bar, there are several tabs: 'Administrators', 'Access Control', 'Authentication', 'SNMP', and 'SNMP Traps'. The 'Administrators' tab is currently selected. The main area of the page is a table with three columns: 'User Name', 'Access Type', and 'Role'. The table is currently empty. At the bottom of the page, there is a search bar with the placeholder text 'Type to search in tables' and a 'Row Count: 0' indicator. On the far right, there are four buttons: 'Add', 'Edit', 'Delete', and 'Exit'.

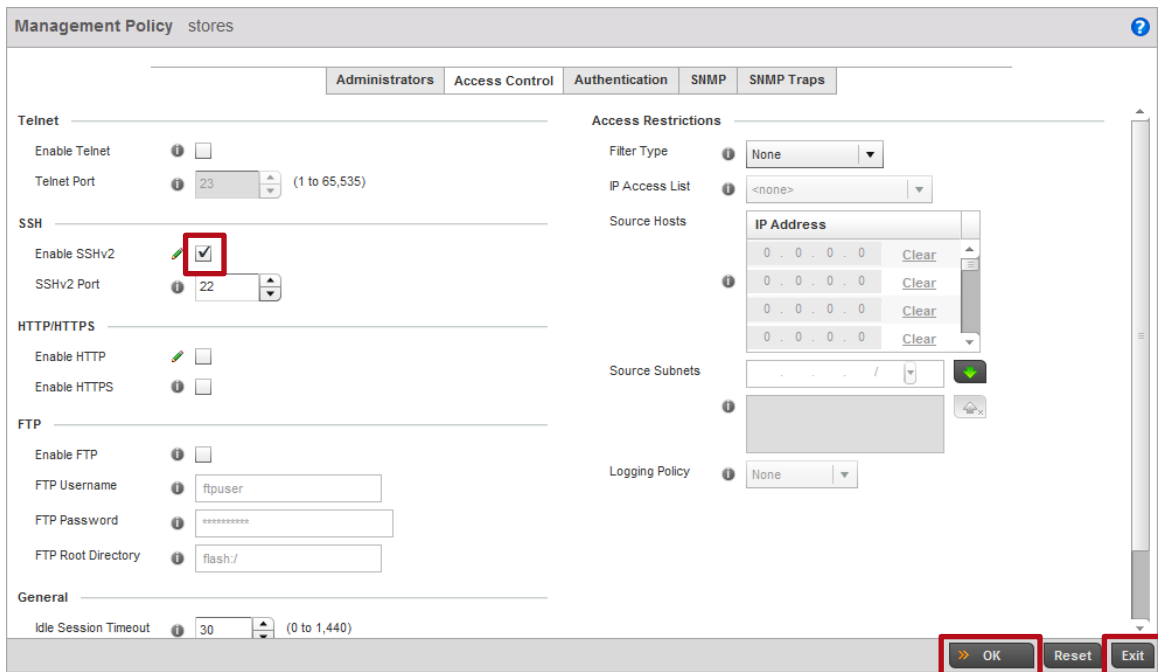
7 Select *Administrators* → *Add*:

The screenshot shows the same 'Management Policy' configuration interface as in the previous step. The 'Management Policy' field now contains 'stores'. The 'Continue' button is no longer highlighted. The 'Add' button in the bottom right corner is now highlighted with a red box. The rest of the interface, including the tabs and the empty table, remains the same.

8 Enter an admin *User Name* and *Password* then select *Role* named *Superuser*. Under *Access Types* select *SSH* then click *OK* and *Exit*:



9 Select *Access Control* tab. Disable *HTTP* then enable the *SSHv2* secure management interface. Click *OK* and *Exit*:



10 User defined Management Policies named *noc* and *stores* have now been defined:

| Management Policy | Telnet | SSHv2 | HTTP | HTTPS | SNMPv2 | SNMPv3 | FTP |
|-------------------|--------|-------|------|-------|--------|--------|-----|
| default           | X      | ✓     | X    | ✓     | X      | ✓      | X   |
| noc               | X      | ✓     | X    | ✓     | ✓      | ✓      | X   |
| stores            | X      | ✓     | X    | X     | ✓      | ✓      | X   |

Type to search in tables Row Count: 3

[Add](#) [Edit](#) [Delete](#)

11 Commit then Save the changes:

WING v5.2 |||| admin

[Revert](#) [Commit](#) [Save](#)

## 2.3 Wireless LANs

Wireless LANs are defined individually within a WiNG 5.X system and can be assigned to groups of Access Point radios using Profiles or to individual Access Point radios as Overrides. Wireless LAN specific parameters such as SSID names and VLAN IDs may also be overridden using Overrides assigned to a RF Domain.

Each Wireless LAN consists of policies and configuration parameters which define the basic operating parameters for the Wireless LAN as well as authentication, encryption, QoS and firewall options. Changes made to a Wireless LANs configuration or assigned policy are automatically inherited by all Access Points serving the Wireless LAN.

No Wireless LANs are pre-defined by default in WiNG 5.X unless they are created using the Initial Configuration Wizard when first initializing a Wireless Controller or Access Point. Wireless LANs can be assigned to groups of Access Point radios using Profiles or to individual Access Point radios as Overrides. Wireless LANs assigned directly to radios as Overrides will supersede any Wireless LANs inherited from a Profile.

In most deployments each remote sites will be servicing the same Wireless LANs allowing the AP6532 user defined Profile to be utilized to assign the Wireless LANs to groups of radios. For deployments where the SSID name or VLAN assignments need to be unique per site, the RF Domain assigned to each site can be provisioned to override the SSID name and/or VLAN assignments for Wireless LANs deployed at that site.

For this configuration step two 802.11i Wireless LANs will be created with the following parameters:

- 1) An AAA Policy named **external-aaa** will be created using centralized AAA servers deployed in the data center / NOC.
- 2) An 802.11i EAP Wireless LAN named **STORES-DOT1X** will be created with the following parameters:
  - a. **EAP** authentication with **CCMP** encryption will be enabled.
  - b. The **AAA Policy** named **external-aaa** assigned.
  - c. **Local** bridging will be enabled and users assigned to the store VLAN **22**.
- 3) An 802.11i PSK Wireless LAN named **STORES-PSK** will be created with the following parameters:
  - a. **PSK** authentication with **CCMP** encryption will be enabled.
  - b. The passphrase will be set to **hellomoto**.
  - c. **Local** bridging will be enabled and users assigned to the store VLAN **23**.

The Wireless LANs named **STORES-DOT1X** and **STORES-PSK** will be assigned to the AP6532 Access Point radios using the user defined Profile named **stores-ap6532**.

## 2.3.1 Command Line Interface

Use the following procedure to create 802.11i Wireless LANs for each store using the Command Line Interface:

### 1 Create a AAA policy named *external-aaa* for the 802.11i EAP Wireless LAN:

```
rfs6000-64435A(config)# aaa-policy external-aaa
```

### 2 Create one or more Authentication server entries. In this example centralized Authentication servers *192.168.10.10* and *192.168.10.11* using no proxy have been defined:

```
rfs6000-64435A(config-aaa-policy-external-aaa)# authentication server 1 host 192.168.10.10 secret hellomoto
rfs6000-64435A(config-aaa-policy-external-aaa)# authentication server 1 proxy-mode none
rfs6000-64435A(config-aaa-policy-external-aaa)# authentication server 2 host 192.168.10.11 secret hellomoto
rfs6000-64435A(config-aaa-policy-external-aaa)# authentication server 2 proxy-mode none
```

### 3 Verify the changes:

```
rfs6000-64435A(config-aaa-policy-external-aaa)# show context

aaa-policy external-aaa
  authentication server 1 host 192.168.10.10 secret 0 hellomoto
  authentication server 1 proxy-mode none
  authentication server 2 host 192.168.10.11 secret 0 hellomoto
  authentication server 2 proxy-mode none
```

### 4 Exit the AAA Policy configuration:

```
rfs6000-64435A(config-aaa-policy-external-aaa)# exit
```

### 5 Create an 802.11i EAP Wireless LAN. In this example the 802.11i EAP Wireless LAN will be named *STORES-DOT1X*:

```
rfs6000-64435A(config)# wlan STORES-DOT1X
```

### 6 Set the *Encryption to CCMP*, *Authentication to EAP* then assign the AAA Server Policy named *external-aaa*. Enable local bridging then assign the local VLAN 22:

```
rfs6000-64435A(config-wlan-STORES-DOT1X)# encryption-type ccmp
rfs6000-64435A(config-wlan-STORES-DOT1X)# authentication-type eap
rfs6000-64435A(config-wlan-STORES-DOT1X)# use aaa-policy external-aaa
rfs6000-64435A(config-wlan-STORES-DOT1X)# bridging-mode local
rfs6000-64435A(config-wlan-STORES-DOT1X)# vlan 22
```

**7 Verify the changes:**

```
rfs6000-64435A(config-wlan-STORES-DOT1X) # show context

wlan STORES-DOT1X
  ssid STORES-DOT1X
  vlan 22
  bridging-mode local
  encryption-type ccmp
  authentication-type eap
  use aaa-policy external-aaa
```

**8 Exit the Wireless LAN configuration:**

```
rfs6000-64435A(config-wlan-STORES-DOT1X) # exit
```

**9 Create a 802.11i PSK Wireless LAN. In this example the 802.11i PSK Wireless LAN will be named STORES-PSK:**

```
rfs6000-64435A(config) # wlan STORES-PSK
```

**10 Set the Encryption to CCMP, Authentication to None then assign a Passphrase. Enable local bridging then assign the local VLAN 23:**

```
rfs6000-64435A(config-wlan-STORES-PSK) # encryption-type ccmp
rfs6000-64435A(config-wlan-STORES-PSK) # authentication-type none
rfs6000-64435A(config-wlan-STORES-PSK) # wpa-wpa2 psk 0 hellomoto
rfs6000-64435A(config-wlan-STORES-PSK) # bridging-mode local
rfs6000-64435A(config-wlan-STORES-PSK) # vlan 23
```

**11 Verify the changes:**

```
rfs6000-64435A(config-wlan-STORES-PSK) # show context

wlan STORES-PSK
  ssid STORES-PSK
  vlan 23
  bridging-mode local
  encryption-type ccmp
  authentication-type none
  wpa-wpa2 psk 0 hellomoto
```

**12 Exit the Wireless LAN configuration then commit and save the changes:**

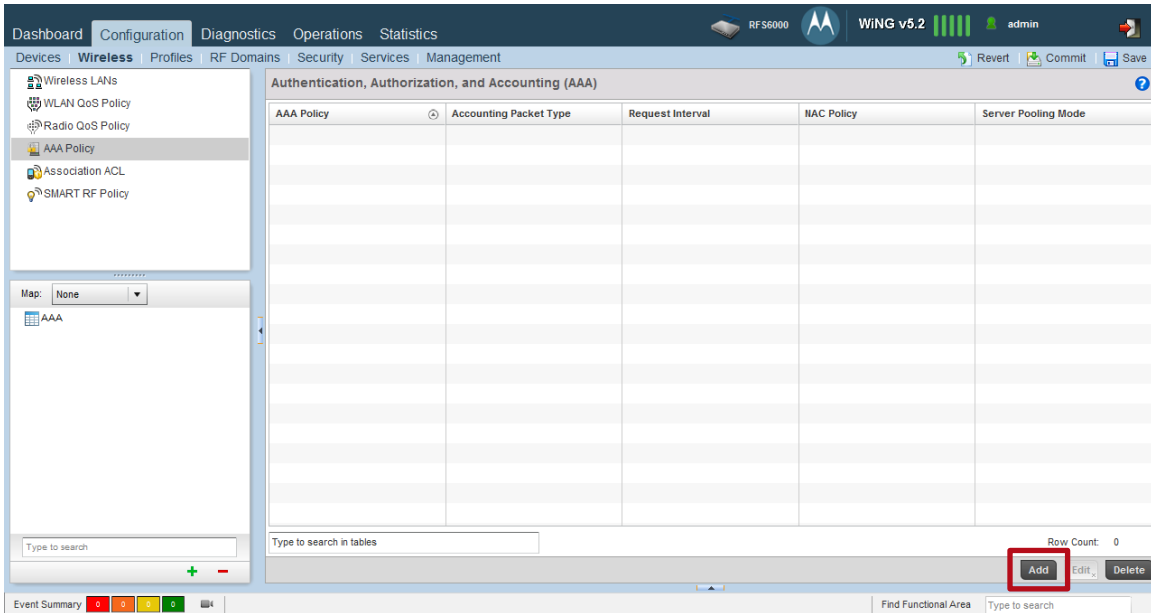
```
rfs6000-64435A(config-wlan-STORES-PSK) # exit
rfs6000-1(config) # commit write

[OK]
```

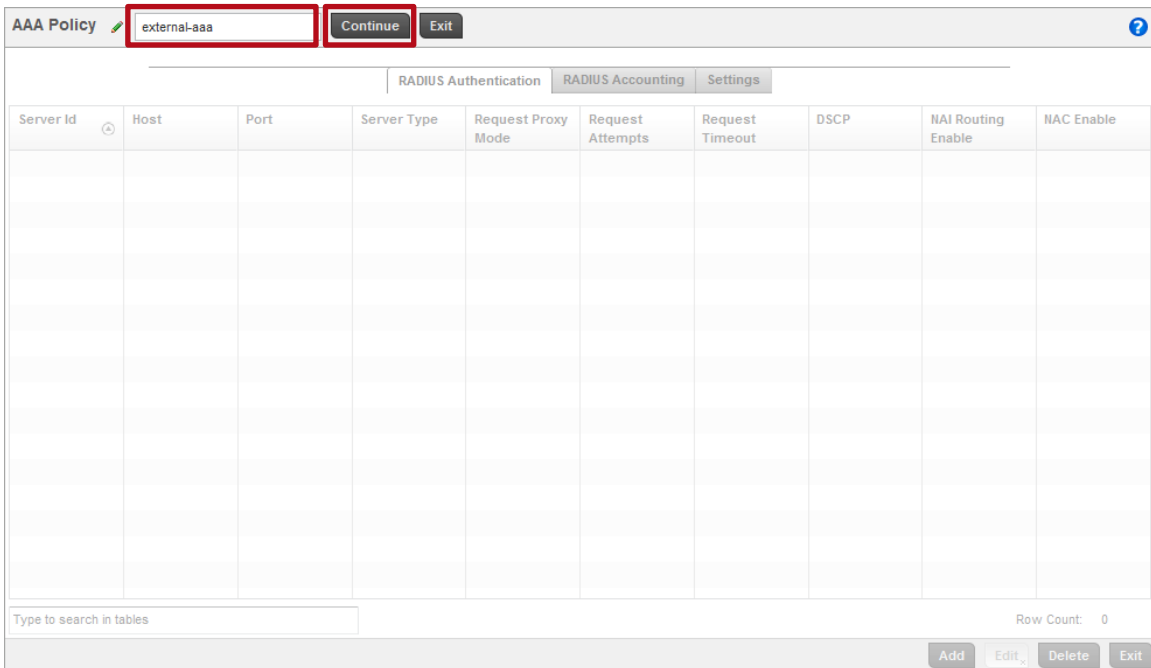
## 2.3.2 Management User Interface

Use the following procedure to create 802.11i Wireless LANs for each store using the Management User Interface:

**1 Select Configuration → Wireless → AAA Policy → Add:**



**2 Enter the Management Policy name external-aaa then click Continue:**







- Click **Add**. Set the **Server Id** to 2 then enter the **IP Address** or **Hostname** of the secondary AAA server. Set the **Server Type** to **Host** then enter the **RADIUS Shared Secret**. Set the **Request Proxy Mode** to **None** then click **OK** and **Exit**:

**Authentication Server**

Server Id: 2 (1 to 6)

**Settings**

Host: 192.168.10.11 (Hostname)

Port: 1812 (1 to 65,535)

Server Type: Host

Secret: hellomoto (Show)

Request Proxy Mode: None

Request Attempts: 3 (1 to 10)

Request Timeout: 3 Seconds (1 to 60)

Retry Timeout Factor: 100 (50 to 200)

DSCP: 46 (0 to 63)

**Network Access Identifier Routing**

NAI Routing Enable:

Realm:

Realm Type:  Prefix  Suffix

Strip Realm:

Buttons: >> OK, Reset, Exit

- Two **RADIUS Authentication** server entries have now been defined in the AAA Server Policy named **external-aaa**. Click **Exit**:

**AAA Policy external-aaa**

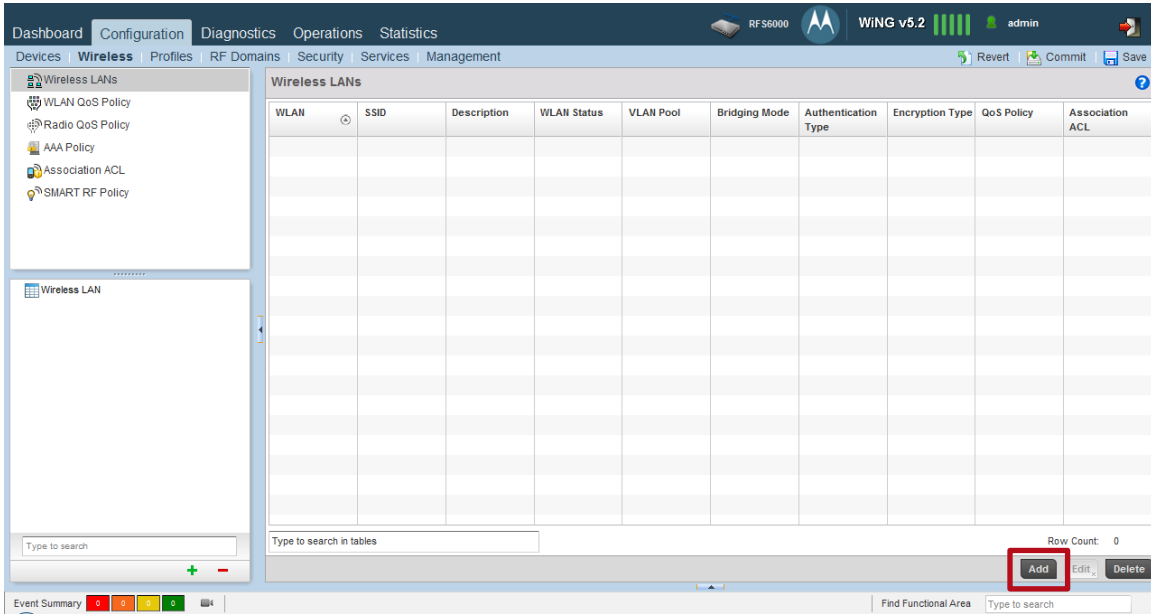
Tab: RADIUS Authentication

| Server Id | Host          | Port  | Server Type | Request Proxy Mode | Request Attempts | Request Timeout | DSCP | NAI Routing Enable | NAC Enable |
|-----------|---------------|-------|-------------|--------------------|------------------|-----------------|------|--------------------|------------|
| 1         | 192.168.10.10 | 1,812 | Host        | None               | 3                | 3s              | 46   | X                  | X          |
| 2         | 192.168.10.11 | 1,812 | Host        | None               | 3                | 3s              | 46   | X                  | X          |

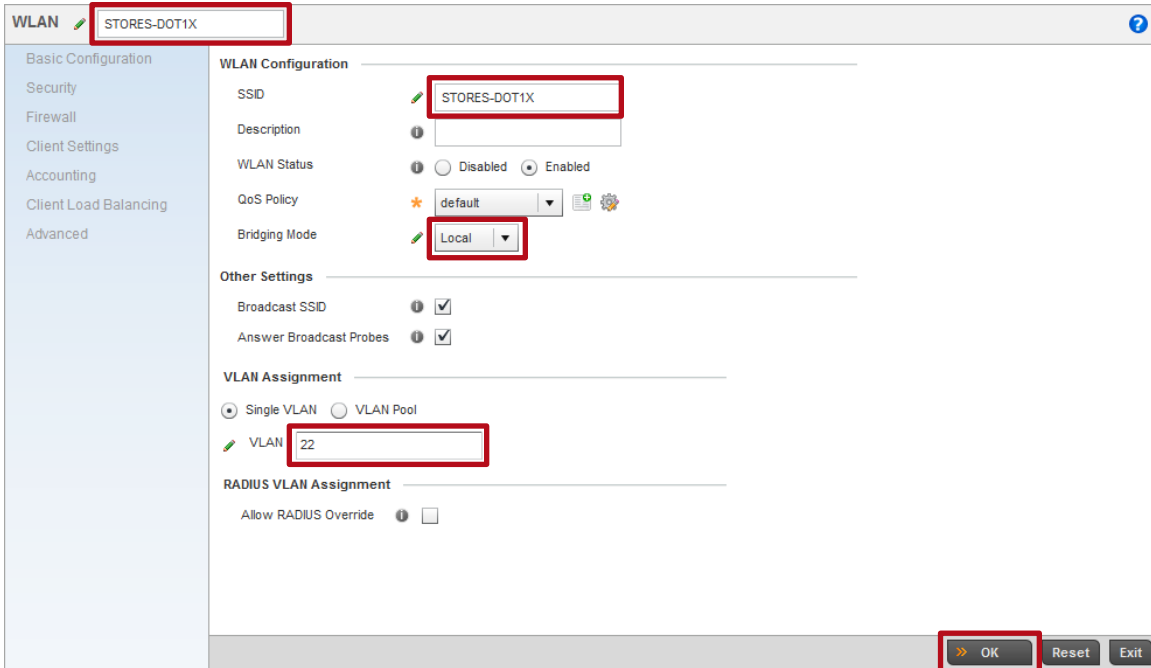
Row Count: 2

Buttons: Add, Edit, Delete, Exit

7 Select Configuration → Wireless → Wireless LANs → Add:



8 Enter the WLAN and SSID name then set the Bridging Mode to Local. Enter the local VLAN ID then click OK. In this example the Wireless LAN will be named STORES-DOT1X and the users mapped to the local VLAN 22:



9 Set the *Authentication Type* to *EAP* then assign the *AAA Policy* named *external-aaa*. Set the *Encryption Type* to *WPA2-CCMP* then click *OK* and *Exit*:

WLAN STORES-DOT1X

Basic Configuration

Security

Firewall

Client Settings

Accounting

Client Load Balancing

Advanced

Select Authentication

Authentication Type  EAP  EAP-PSK  EAP-MAC  MAC  Kerberos  PSK / None

Kerberos Configuration [Settings](#)

AAA Policy  external-aaa

Reauthentication  30 (30 to 86,400)

Captive Portal

Enforcement  Captive Portal Enable  Captive Portal if Primary Authentication Fails

Captive Portal Policy

Select Encryption

WPA/WPA2-TKIP  WEP 128  WEP 64  Open

WPA2-CCMP  KeyGuard

Key Settings

Enter 64 HEX or 8-63 ASCII Characters

Pre-Shared Key  ASCII

OK Reset Exit

10 Click *Add* to create a second Wireless LAN:

Wireless LANs

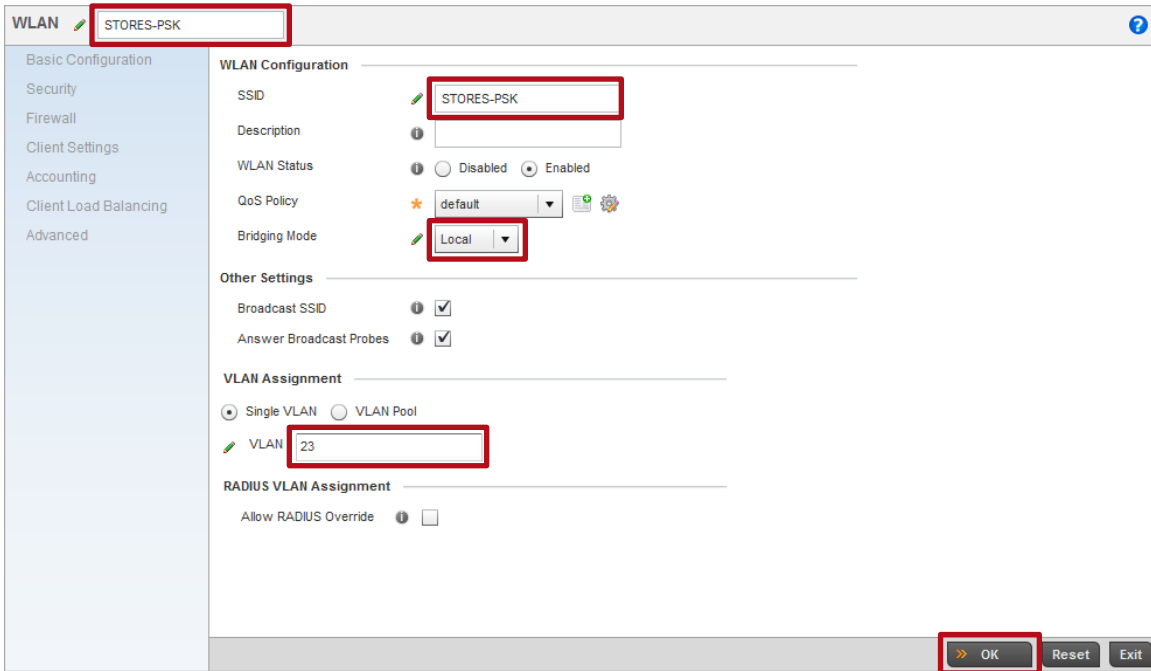
| WLAN         | SSID         | Description | WLAN Status | VLAN Pool | Bridging Mode | Authentication Type | Encryption Type | QoS Policy | Association ACL |
|--------------|--------------|-------------|-------------|-----------|---------------|---------------------|-----------------|------------|-----------------|
| STORES-DOT1X | STORES-DOT1X |             | Enabled     | 22        | Local         | EAP                 | CCMP            | default    |                 |

Type to search in tables

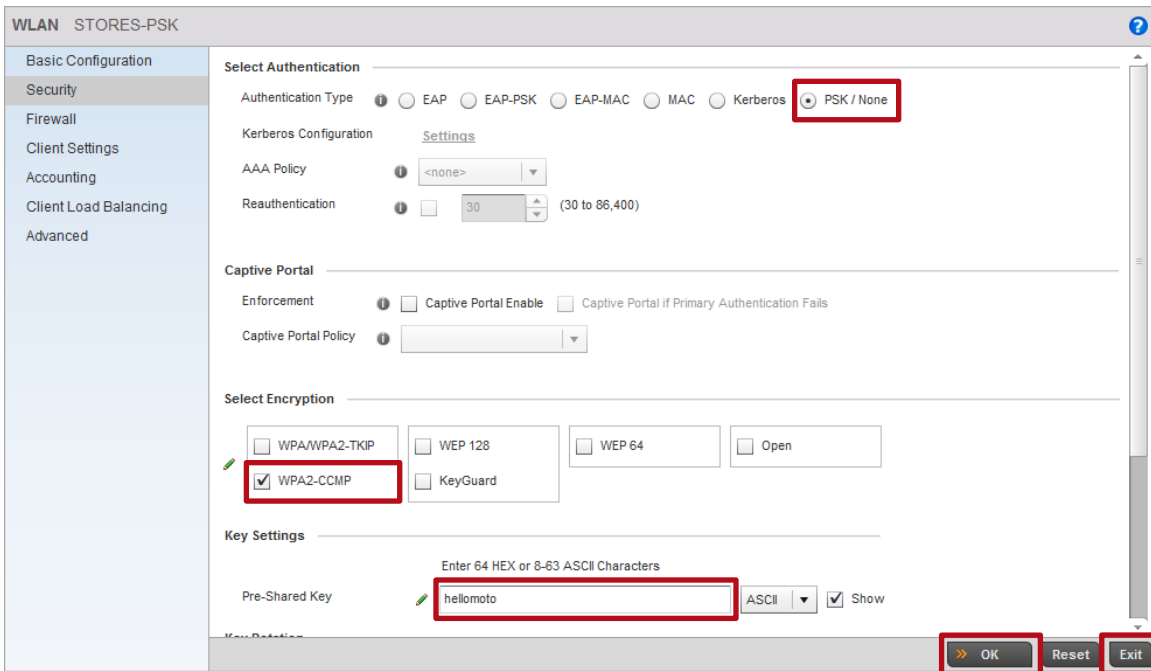
Row Count: 1

Add Edit Delete

11 Enter the *WLAN* and *SSID* name then set the *Bridging Mode* to *Local*. Enter the local *VLAN ID* then click *OK*. In this example the Wireless LAN will be named *STORES-PSK* and the users mapped to the local *VLAN 23*:



12 Set the *Authentication Type* to *PSK/None* then set the *Encryption Type* to *WPA2-CCMP*. In the *Pre-Shared Key* field enter *hellomoto* then click *OK* and *Exit*:





## 2.4 Profiles

Profiles allow common configuration parameters and Policies to be assigned to groups of Wireless Controllers and Access Points. Profiles are Wireless Controller and Access Point model specific and a Wireless Controller or Access Point can only be assigned to a Profile defined for its hardware type.

Profiles allow common configuration parameters and policies to be assigned to groups of managed devices such as the Wireless Controllers in the data center / NOC or remote Access Points. Changes made to a Profile are automatically inherited by the devices assigned to that profile allowing new services to be quickly deployed in the data center / NOC or remote sites.

By default Controllers and Access Points are automatically assigned to a default device Profile based on their hardware type (example default-rfs6000, default-rfs7000, default-ap6532 etc.). Administrators may optionally create user defined profiles which can be manually assigned to existing devices or automatically assigned to new devices using Automatic Provisioning Policies. Each WiNG 5.X device must be assigned to a default or user defined Profile!

In this data center / NOC deployment example the Wireless Controllers and remote Access Points share common configuration parameters such as Management Policies, VLAN port assignments, Wireless LANs, DNS and NTP servers. To assign these common configuration parameters a user defined Profile will be created and manually assigned to the Wireless Controllers in the data center / NOC while a user defined Profile will be created and automatically assigned to remote Access Points using Automatic Provisioning Policies.

For this configuration step two user defined Profiles will be created with the following parameters:

- 1) A user defined RFS6000 device Profile named **noc-rfs6000** will be created for the Wireless Controllers in the data center / NOC with the following parameters:
  - a. The user defined **Management Policy** named **noc** will be assigned.
  - b. The **up1** port will be configured as a **Trunk** port with the tagged Native VLAN ID **20**.
  - c. The **Domain Name** will be set to **tmelabs.local** and the **Name Server** address **192.168.10.5** defined.
  - d. A **NTP** server **192.168.10.5** will be assigned.
- 2) A user defined AP6532 device Profile named **stores-ap6532** will be created for the remote Access Points with the following parameters:
  - a. The user defined **Management Policy** named **stores** will be assigned.
  - b. The **ge1** port will be configured as a **Trunk** port with the untagged Native VLAN ID **21** and tagged user VLAN IDs **22** and **23**.
  - c. Create a **Virtual IP Interface** for the Native VLAN ID **21** with the **DHCP Client** enabled.
  - d. The Wireless LAN named **STORES-DOT1X** will be assigned to both **radio1** and **radio2** while the Wireless LAN named **STORES-PSK** will only be assigned to **radio1**.
  - e. The **Domain Name** will be set to **tmelabs.local** and the **Name Server** address **192.168.10.5** defined.
  - f. A **NTP** server **192.168.10.5** will be assigned.

The user defined Profile named **noc-rfs6000** will be manually assigned to each RFS6000 Wireless Controller using Device configuration while the user defined Profile named **stores-ap6532** will be automatically assigned to each remote Access Point as they are discovered and adopted using an Automatic Provisioning Policy. The Automatic Provisioning Policy will be assigned to the user defined Profile named **noc-rfs6000** in a later step.



Note – As a best practice it is recommended that the Wireless Controllers be connected to the network using 802.1Q tagging which allows additional VLANs to be added in the future without disrupting the Wireless network. As an industry best practice it is also recommended that the Native VLAN is tagged.



Note – It is highly recommended that the Access Points Native VLAN id match the VLAN id of the switch port that the Access Point is connected to at the remote site.

## 2.4.1 Command Line Interface

Use the following procedure to create a user defined device Profiles for the Wireless Controllers in the data center / NOC and the remote Access Points for each store using the Command Line Interface:

### 1 Create a RFS6000 user defined Profile for the Wireless Controllers in the data center named *noc-rfs6000*:

```
rfs6000-64435A(config)# profile rfs6000 noc-rfs6000
rfs6000-64435A(config-profile-noc-rfs6000)#
```

### 2 Assign the user defined Management policy named *noc*:

```
rfs6000-64435A(config-profile-noc-rfs6000)# use management-policy noc
```

### 3 Configure *up1* as a *Trunk* port and assign the tagged Native VLAN 20:

```
rfs6000-64435A(config-profile-noc-rfs6000)# interface up1
rfs6000-64435A(config-profile-noc-rfs6000-if-up1)# description Uplink
rfs6000-64435A(config-profile-noc-rfs6000-if-up1)# switchport mode trunk
rfs6000-64435A(config-profile-noc-rfs6000-if-up1)# switchport trunk native vlan 20
rfs6000-64435A(config-profile-noc-rfs6000-if-up1)# switchport trunk allowed vlan 20
rfs6000-64435A(config-profile-noc-rfs6000-if-up1)# switchport trunk native tagged
rfs6000-64435A(config-profile-noc-rfs6000-if-up1)# exit
```

### 4 Assign a *Domain Name*, *Name Server* and *NTP Server*:

```
rfs6000-64435A(config-profile-noc-rfs6000)# ip domain-name tmelabs.local
rfs6000-64435A(config-profile-noc-rfs6000)# ip name-server 192.168.10.5
rfs6000-64435A(config-profile-noc-rfs6000)# ntp server 192.168.10.5
```

### 5 Verify the changes:

```
rfs6000-64435A(config-management-policy-noc)# show context

profile rfs6000 noc-rfs6000
ip name-server 192.168.10.5
ip domain-name tmelabs.local
!
! Unnecessary configuration omitted for brevity
!
interface up1
```

```

description Uplink
switchport mode trunk
switchport trunk native vlan 20
switchport trunk native tagged
switchport trunk allowed vlan 20
ip dhcp trust
qos trust dscp
qos trust 802.1p
!
! Unnecessary configuration omitted for brevity
!
use management-policy noc
use firewall-policy default
ntp server 192.168.10.5
service pm sys-restart

```

## 6 Exit the Profile configuration:

```
rfs6000-64435A(config-profile-noc-rfs6000)# exit
```

## 7 Create a AP6532 user defined Profile for the remote Access Points named *stores-ap6532*

```

rfs6000-64435A(config)# profile ap6532 stores-ap6532
rfs6000-64435A(config-profile-stores-ap6532)#

```

## 8 Assign the user defined Management policy named *stores*:

```
rfs6000-64435A(config-profile-stores-ap6532)# use management-policy stores
```

## 9 Configure *ge1* as a *Trunk* port and assign the untagged Native VLAN 21 and tagged user VLANs 22 and 23:

```

rfs6000-64435A(config-profile-stores-ap6532)# interface ge1
rfs6000-64435A(config-profile-stores-ap6532-if-ge1)# description Uplink
rfs6000-64435A(config-profile-stores-ap6532-if-ge1)# switchport mode trunk
rfs6000-64435A(config-profile-stores-ap6532-if-ge1)# switchport trunk native vlan 21
rfs6000-64435A(config-profile-stores-ap6532-if-ge1)# switchport trunk allowed vlan 21-23
rfs6000-64435A(config-profile-stores-ap6532-if-ge1)# exit

```

## 10 Create a *Virtual IP* interface on the Native VLAN 21 with the *DHCP* client enabled. This is required so that the Access Points at the site can automatically boot and discover the Wireless Controllers in the data center / NOC using DHCP:

```

rfs6000-64435A(config-profile-stores-ap6532)# interface vlan21
rfs6000-64435A(config-profile-stores-ap6532-if-vlan21)# description AP\ VLAN
rfs6000-64435A(config-profile-stores-ap6532-if-vlan21)# ip address dhcp
rfs6000-64435A(config-profile-stores-ap6532-if-vlan21)# ip dhcp client request options all
rfs6000-64435A(config-profile-stores-ap6532-if-vlan21)# exit

```



### 11 Assign Wireless LANs to the 2.4 GHz radio1. In this example the Wireless LANs named *STORES-DOT1X* and *STORES-PSK* are assigned to the 2.4 GHz radios:

```
rfs6000-64435A(config-profile-stores-ap6532)# interface radio 1
rfs6000-64435A(config-profile-stores-ap6532-if-radio1)# wlan STORES-DOT1X
rfs6000-64435A(config-profile-stores-ap6532-if-radio1)# wlan STORES-PSK
rfs6000-64435A(config-profile-stores-ap6532-if-radio1)# exit
```

### 12 Assign Wireless LANs to the 5 GHz radio1. In this example only the Wireless LAN named *STORES-DOT1X* is assigned to the 5 GHz radios:

```
rfs6000-64435A(config-profile-stores-ap6532)# interface radio 2
rfs6000-64435A(config-profile-stores-ap6532-if-radio2)# wlan STORES-DOT1X
rfs6000-64435A(config-profile-stores-ap6532-if-radio2)# exit
```

### 13 Assign a Domain Name, Name Server and NTP Server:

```
rfs6000-64435A(config-profile-stores-ap6532)# ip domain-name tmelabs.local
rfs6000-64435A(config-profile-stores-ap6532)# ip name-server 192.168.10.5
rfs6000-64435A(config-profile-stores-ap6532)# ntp server 192.168.10.5
```

### 14 Verify the changes:

```
rfs6000-64435A(config-profile-stores-ap6532)# show context
```

```
profile ap6532 stores-ap6532
 ip name-server 192.168.10.5
 ip domain-name tmelabs.local
 no autoinstall configuration
 no autoinstall firmware
 interface radio1
  wlan STORES-PSK bss 1 primary
  wlan STORES-DOT1X bss 2 primary
 interface radio2
  wlan STORES-DOT1X bss 1 primary
 interface ge1
  description Uplink
  switchport mode trunk
  switchport trunk native vlan 21
  no switchport trunk native tagged
  switchport trunk allowed vlan 21-23
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface vlan21
  description AP\ VLAN
  ip address dhcp
  ip dhcp client request options all
```

```
use management-policy stores
use firewall-policy default
ntp server 192.168.10.5
service pm sys-restart
```

**15 Exit the Profile configuration then *commit* and save the changes:**

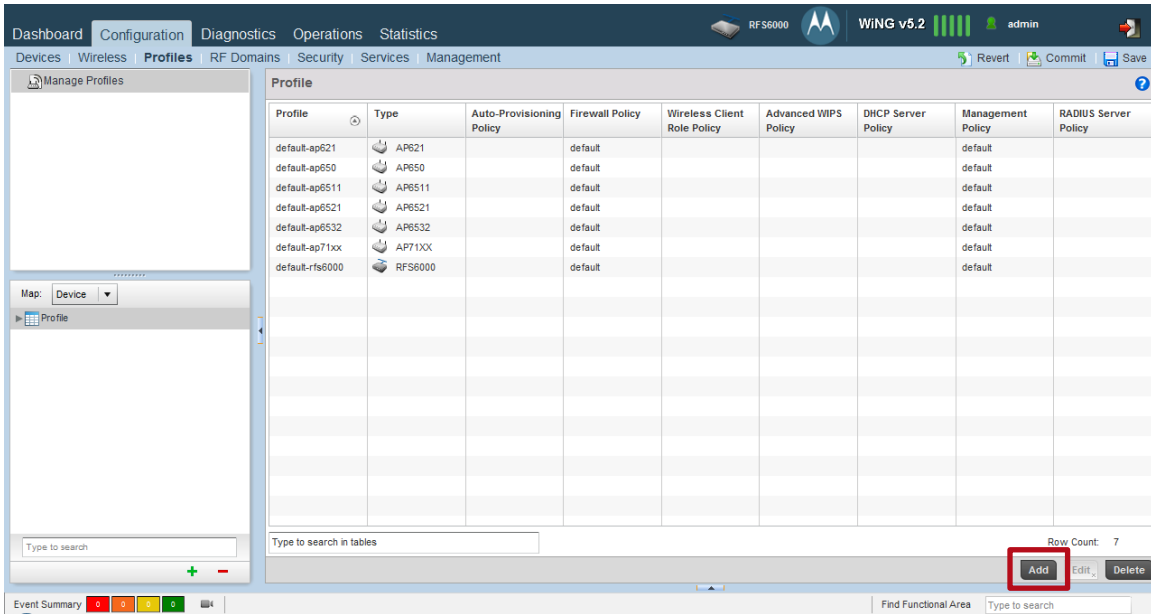
```
rfs6000-64435A(config-profile-stores-ap6532) # exit
rfs6000-64435A(config) # commit write

[OK]
```

## 2.4.2 Management User Interface

Use the following procedure to create a user defined device Profiles for the Wireless Controllers in the data center / NOC and the remote Access Points for each store using the Management User Interface:

**1 Select Configuration → Profiles → Add:**



2 Type the *Profile* name *rfs6000-noc* then set the *Type* to *rfs6000*. Under *Network Time Protocol* click *Add Row* then enter the *NTP Server IP Address*. Click *OK*:

The screenshot shows the configuration page for profile 'noc-rfs6000' of type 'RFS6000'. Under the 'Network Time Protocol (NTP)' section, there is a table with the following data:

| Server IP    | Authentication Key | Prefer                   | Autokey                  | Key | Version |
|--------------|--------------------|--------------------------|--------------------------|-----|---------|
| 192.168.10.5 | 0                  | <input type="checkbox"/> | <input type="checkbox"/> |     | 0       |

The 'Add Row' button is located below the table. At the bottom of the page, there are 'OK', 'Reset', and 'Exit' buttons.

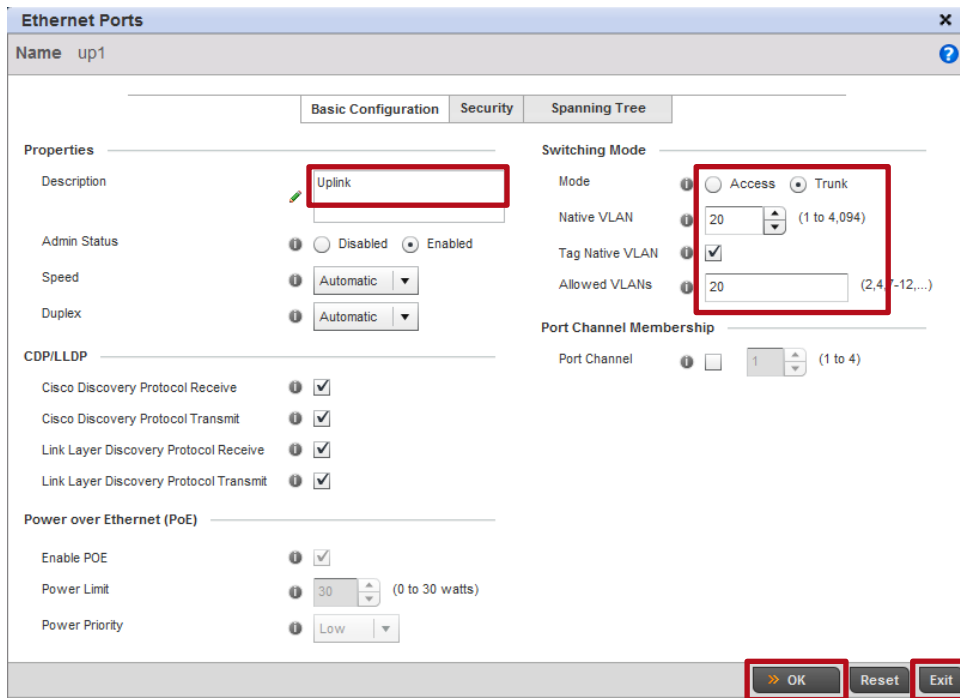
3 Select *Interface* → *Ethernet Ports* → *up1* → *Edit*:

The screenshot shows the configuration page for profile 'noc-rfs6000' of type 'RFS6000'. The 'Interface' section is expanded to show 'Ethernet Ports'. The following table lists the interfaces:

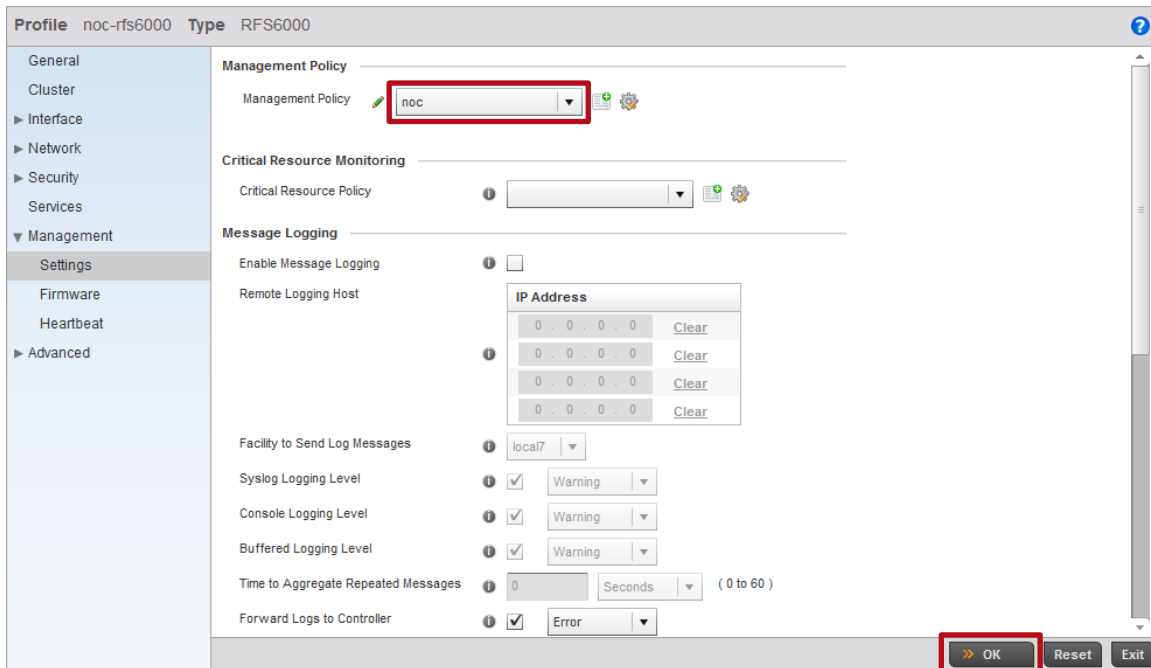
| Name | Type     | Description | Admin Status | Mode   | Native VLAN | Tag Native VLAN | Allowed VLANs |
|------|----------|-------------|--------------|--------|-------------|-----------------|---------------|
| ge1  | Ethernet |             | ✓ Enabled    | Access | 1           | ✗               |               |
| ge2  | Ethernet |             | ✓ Enabled    | Access | 1           | ✗               |               |
| ge3  | Ethernet |             | ✓ Enabled    | Access | 1           | ✗               |               |
| ge4  | Ethernet |             | ✓ Enabled    | Access | 1           | ✗               |               |
| ge5  | Ethernet |             | ✓ Enabled    | Access | 1           | ✗               |               |
| ge6  | Ethernet |             | ✓ Enabled    | Access | 1           | ✗               |               |
| ge7  | Ethernet |             | ✓ Enabled    | Access | 1           | ✗               |               |
| ge8  | Ethernet |             | ✓ Enabled    | Access | 1           | ✗               |               |
| me1  | Ethernet |             | ✓ Enabled    | Access | 1           | ✗               |               |
| up1  | Ethernet |             | ✓ Enabled    | Access | 1           | ✗               |               |

The 'up1' interface is highlighted with a red border. At the bottom right, there are 'Edit' and 'Exit' buttons.

- 4 Enter a *Description* then set the *Switching Mode* to *Trunk*. Enter the *Native VLAN* and *Allowed VLANs*. Select the option *Tag Native VLAN* then click *OK* and *Exit*. Note in this example tagged VLAN 20 is deployed in the data center NOC:



- 5 Select *Management* → *Settings*. Assign the user defined *Management Policy* named *noc* then click *OK*:



6 Select *Network* → *DNS*. Assign the *Domain Name* then enter the *Name Server IP address*. Click *OK* then *Exit*:

Profile noc-rfs6000 Type RFS6000

**Domain Name System (DNS)**

Domain Name: tmelabs.local

Enable Domain Lookup:

DNS Server Forwarding:

**DNS Servers**

Name Servers

| IP Address   | Clear |
|--------------|-------|
| 192.168.10.5 | Clear |
| 0.0.0.0      | Clear |
| 0.0.0.0      | Clear |

Buttons: OK, Reset, Exit

7 A user defined *Profile* named *noc-rfs6000* has now been created:

| Profile         | Type    | Auto-Provisioning Policy | Firewall Policy | Wireless Client Role Policy | Advanced WIPS Policy | DHCP Server Policy | Management Policy | RADIUS Server Policy |
|-----------------|---------|--------------------------|-----------------|-----------------------------|----------------------|--------------------|-------------------|----------------------|
| default-ap621   | AP621   |                          | default         |                             |                      |                    | default           |                      |
| default-ap650   | AP650   |                          | default         |                             |                      |                    | default           |                      |
| default-ap6511  | AP6511  |                          | default         |                             |                      |                    | default           |                      |
| default-ap6521  | AP6521  |                          | default         |                             |                      |                    | default           |                      |
| default-ap6532  | AP6532  |                          | default         |                             |                      |                    | default           |                      |
| default-ap71xx  | AP71XX  |                          | default         |                             |                      |                    | default           |                      |
| default-rfs6000 | RFS6000 |                          | default         |                             |                      |                    | default           |                      |
| noc-rfs6000     | RFS6000 |                          | default         |                             |                      |                    | noc               |                      |

Row Count: 8

Buttons: Add, Edit, Delete



10 Type the *Profile* name *ap6532-stores* then set the *Type* to *ap6532*. Under *Network Time Protocol* click *Add Row* then enter the *NTP Server IP Address*. Click *OK*:

The screenshot shows the configuration page for a profile named 'stores-ap6532' of type 'AP6532'. The left sidebar lists various configuration categories like General, Power, Cluster, Adoption, Interface, Network, Security, Services, Management, and Advanced. The main content area is divided into sections: Settings (with IP Routing checked), AP300 Adoption (with 'Adopt Unknown APs Automatically' checked), and Network Time Protocol (NTP). The NTP section contains a table with the following data:

| Server IP    | Authentication Key | Prefer                   | Autokey                  | Key | Version |  |
|--------------|--------------------|--------------------------|--------------------------|-----|---------|--|
| 192.168.10.5 | 0                  | <input type="checkbox"/> | <input type="checkbox"/> |     | 0       |  |

Below the table is an 'Add Row' button. At the bottom right of the configuration area are 'OK', 'Reset', and 'Exit' buttons.

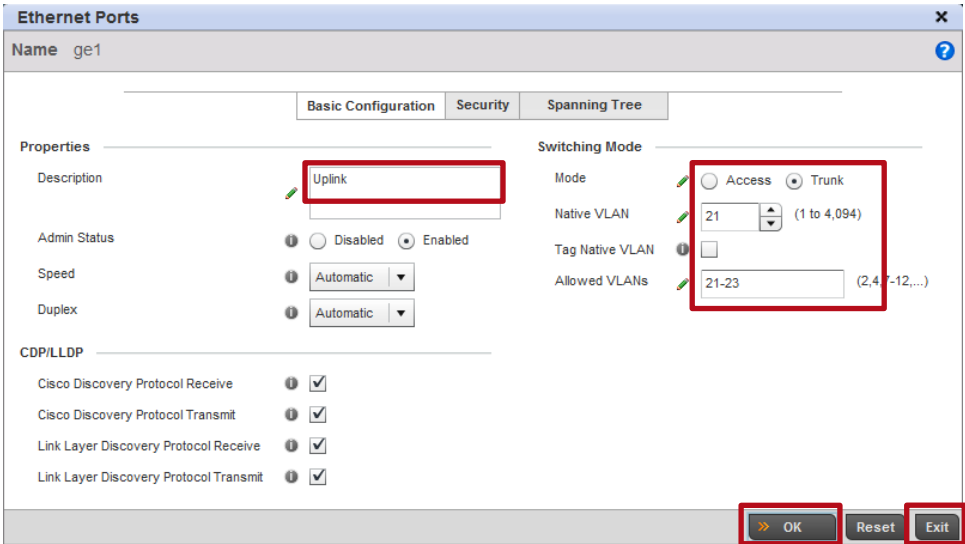
11 Select *Interface* → *Ethernet Ports* → *ge1* → *Edit*:

The screenshot shows the configuration page for the profile 'stores-ap6532' of type 'AP6532'. The left sidebar is expanded to 'Interface' → 'Ethernet Ports'. The main content area displays a table with the following data:

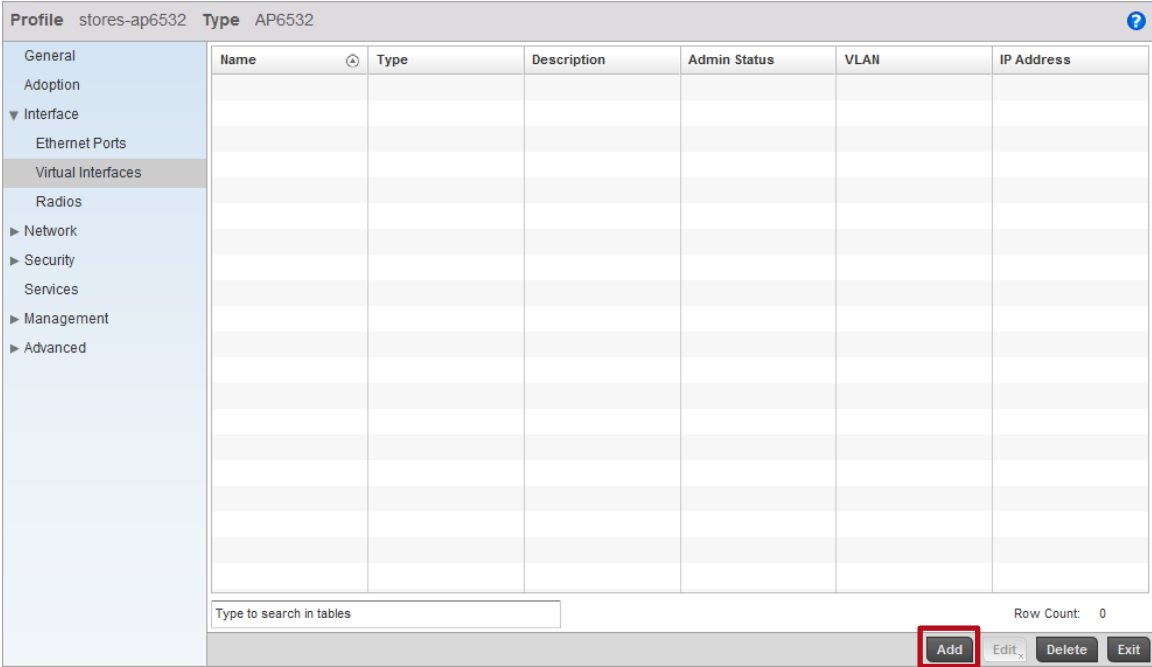
| Name | Type     | Description | Admin Status | Mode   | Native VLAN | Tag Native VLAN | Allowed VLANs |
|------|----------|-------------|--------------|--------|-------------|-----------------|---------------|
| ge1  | Ethernet |             | Enabled      | Access | 1           |                 |               |

At the bottom right of the table area, there is a search bar and a 'Row Count: 1' indicator. Below the table are 'Edit' and 'Exit' buttons.

12 Enter a *Description* then set the *Switching Mode* to *Trunk* and enter the *Native VLAN* and *Allowed VLANs*. Click *OK* and *Exit*. Note in this example the untagged Native VLAN 21 and tagged user VLANs 22 and 23 are deployed in each of the remote stores:



13 Select *Interface* → *Virtual Interfaces* → *Add*:





14 In the *VLAN ID* field enter the *Native VLAN* for the stores then select the options *Use DHCP to Obtain IP* and *Use DHCP to obtain Gateway / DNS Servers*. Click *OK*. Note in this example the Native ID for all the remote stores is VLAN 21:

**Virtual Interfaces**

VLAN ID: 21 (1 - 4,094)

**Properties**

Description: AP VLAN

Admin Status: Disabled / Enabled

**IP Addresses**

Enable Zero Configuration: None / Primary / Secondary

Primary IP Address: [Empty]

Use DHCP to obtain Gateway/DNS Servers: [Checked] (Allowed on 1 virtual interface)

Secondary Addresses: [Empty]

**DHCP Relay**

Respond to DHCP Relay Packets: [Unchecked]

DHCP Relays:

| IP Address    | Clear |
|---------------|-------|
| 0 . 0 . 0 . 0 | Clear |
| 0 . 0 . 0 . 0 | Clear |
| 0 . 0 . 0 . 0 | Clear |
| 0 . 0 . 0 . 0 | Clear |

**Network Address Translation (NAT)**

NAT Direction: Inside / Outside / None

Buttons: OK, Reset, Exit

15 Select *Interface* → *Radios* → *radio1* → *Edit*.

Profile: stores-ap6532 Type: AP6532

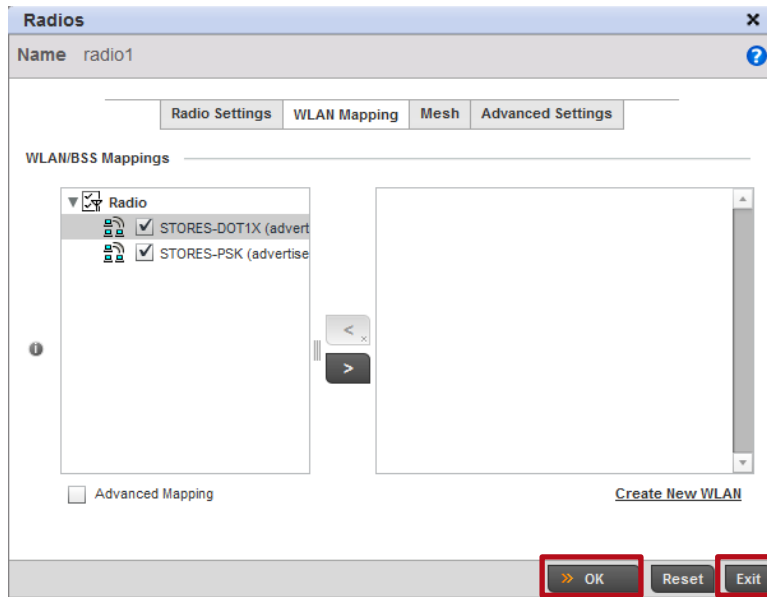
| Name   | Type  | Description | Admin Status | RF Mode      | Channel | Transmit Power |
|--------|-------|-------------|--------------|--------------|---------|----------------|
| radio1 | Radio | radio1      | Enabled      | 2.4 GHz WLAN | smart   | smart          |
| radio2 | Radio | radio2      | Enabled      | 5 GHz WLAN   | smart   | smart          |

Type to search in tables

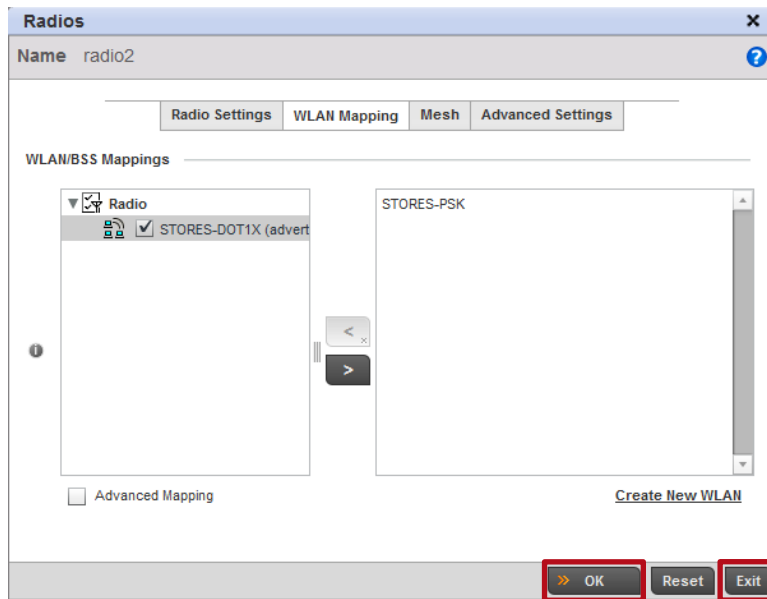
Row Count: 2

Buttons: Edit, Exit

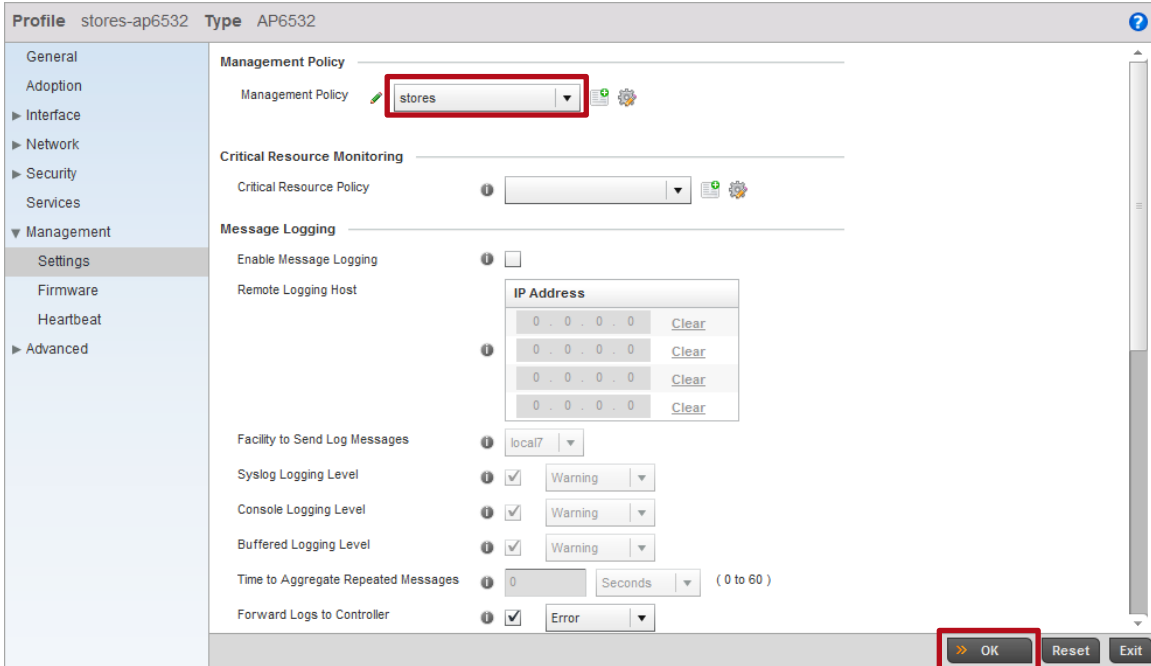
- 16 Select *WLAN Mapping* then select and *Add* one or more Wireless LANs to the 2.4 GHz radio. Click *OK* then *Exit*. Note in this example the Wireless LANs named *STORES-DOT1X* and *STORES-PSK* have been assigned to the 2.4 GHz radio:



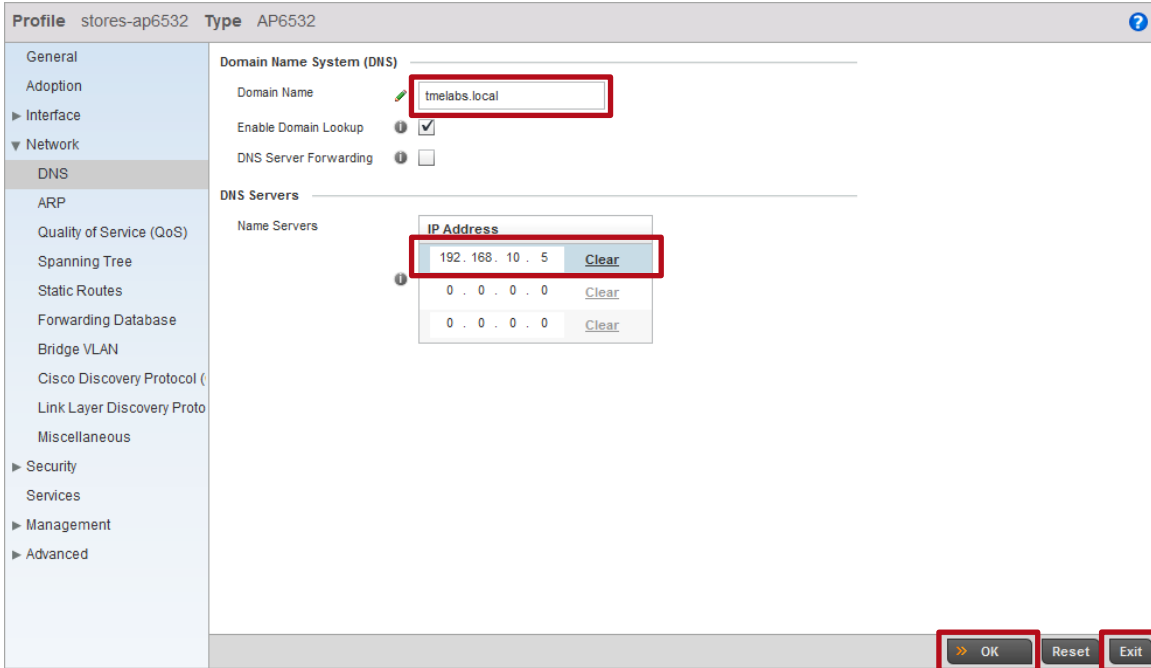
- 17 Select *radio2* then click *Edit*. Select *WLAN Mapping* then select and *Add* one or more Wireless LANs to the 5 GHz radio. Click *OK* then *Exit*. Note in this example the Wireless LAN named *STORES-DOT1X* has been assigned to the 5 GHz radio:



18 Select *Management* → *Settings*. Assign the user defined *Management Policy* named *stores* then click *OK*:



19 Select *Network* → *DNS*. Assign the *Domain Name* then enter the *Name Server IP address*. Click *OK* then *Exit*:





## 2.5 Overrides

In the previous step we defined a user defined Profiles which assigned common configuration parameters to the Wireless Controllers in the data center / NOC and the remote Access Points. Device configuration allows configuration parameters and Policies to be assigned to individual devices which are referred to as Overrides. Overrides allow device specific parameters such as static IP addresses, cluster configuration parameters and hostnames to be assigned to individual devices. In Configuration parameters and Policies can be defined that Override specific configuration parameters and Policies inherited from a Profile.

### 2.5.1 Wireless Controller (Cluster Master)

For this configuration step the Wireless Controller that is designated as the Cluster Master will be assigned the following Device Configuration:

- 1) The default VLAN 1 will be removed (not applicable for the RFS7000 or NX9000).
- 2) The user defined **Profile** named **noc-rfs6000** will be assigned.
- 3) The user defined **RF Domain** named **noc** will be assigned.
- 4) The **Hostname** will be set to **rfs6000-1**.
- 5) A **Virtual IP Interface** for **VLAN 20** will be created and the static IP address **192.168.20.23/24** assigned.
- 6) A default route pointing to **192.168.20.1** will be defined.
- 7) The cluster name will be set to **noc**.
- 8) The cluster priority will be set to **255** (highest value becomes the master).
- 9) A **Level 2 IP MINT Link** will be defined pointing to the Cluster Members IP address **192.168.20.23**.

#### 2.5.1.1 Command Line Interface

Use the following procedure to modify the Device configuration for the Cluster Master controller using the Command Line Interface:

##### 1 Access the Device configuration of the Cluster Master and assign the user defined RF Domain named **noc** and user defined Profile named **rfs6000-noc**:

```
rfs6000-64435A(config)# self

rfs6000-64435A(config-device-00-23-68-64-43-5A)# use profile noc-rfs6000
rfs6000-64435A(config-device-00-23-68-64-43-5A)# use rf-domain noc
```

##### 2 If applicable remove the default Virtual IP Interface for VLAN 1:

```
rfs6000-64435A(config-device-00-23-68-64-43-5A)# remove-override interface vlan 1
```

##### 3 Define a **Hostname** for the device. Note in this example the hostname **rfs6000-1** is assigned:

```
rfs6000-64435A(config-device-00-23-68-64-43-5A)# hostname rfs6000-1
```

- 4 Create a *Virtual IP Interface* for the Native VLAN and assign a static IP address. Note in this example a Virtual IP interface for VLAN 20 has been created and the static IP address 192.168.20.22/24 assigned:**

```
rfs6000-64435A(config-device-00-23-68-64-43-5A) # interface vlan 20
rfs6000-64435A(config-device-00-23-68-64-43-5A-if-vlan20) # description Management
rfs6000-64435A(config-device-00-23-68-64-43-5A-if-vlan20) # ip address 192.168.20.22/24
rfs6000-64435A(config-device-00-23-68-64-43-5A-if-vlan20) # exit
```

- 5 Assign a default gateway. Note in this example the default gateway for VLAN 20 is 192.168.20.1:**

```
rfs6000-64435A(config-device-00-23-68-64-43-5A) # ip route 0.0.0.0/0 192.168.20.1
```

- 6 Define a *Cluster Name*, *Cluster Member IP Address* and set the *Cluster Priority* to 255 (Master). Note in this example the *Cluster Name* is set to *noc* and the Cluster Members IP address is 192.168.20.23. In addition the MINT link level between the cluster peers is set to *Level 2*:**

```
rfs6000-64435A(config-device-00-23-68-64-43-5A) # cluster name noc
rfs6000-64435A(config-device-00-23-68-64-43-5A) # cluster member ip 192.168.20.23 level 2
rfs6000-64435A(config-device-00-23-68-64-43-5A) # cluster master-priority 255
```

- 7 Verify the changes:**

```
rfs6000-64435A(config-device-00-23-68-64-43-5A) # show context

rfs6000 00-23-68-64-43-5A
use profile noc-rfs6000
use rf-domain noc
hostname rfs6000-1
!
! Unnecessary configuration omitted for brevity
!
ip default-gateway 192.168.20.1
interface vlan20
description Management
ip address 192.168.20.22/24
cluster name noc
cluster member ip 192.168.20.23 level 2
cluster master-priority 255
logging on
logging console warnings
logging buffered warnings
```

- 8 Exit the Profile configuration then *commit* and save the changes:**

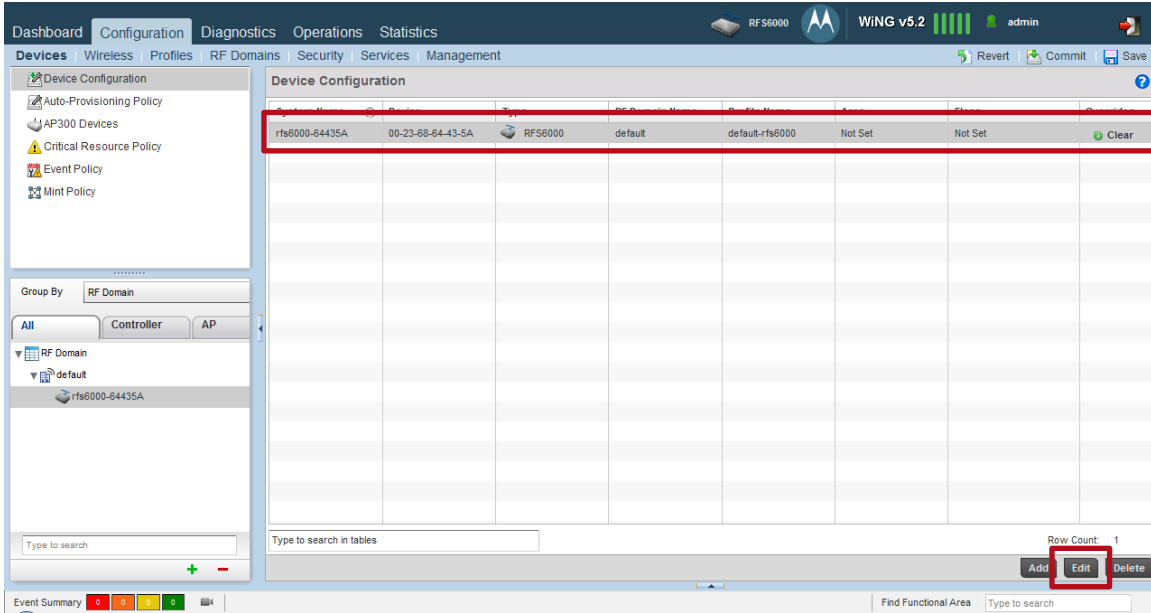
```
rfs6000-64435A(config-device-00-23-68-64-43-5A) # exit
rfs6000-64435A(config) # commit write
```

[OK]

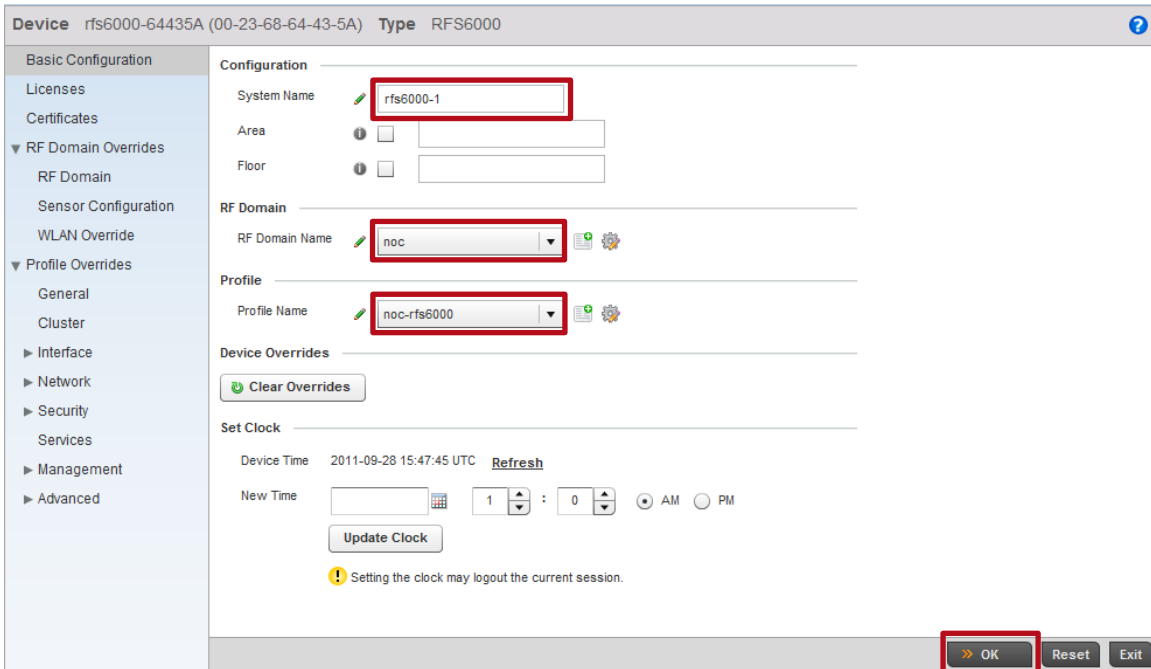
## 2.5.1.2 Management User Interface

Use the following procedure to modify the Device configuration for the Cluster Master controller using the Management User Interface:

**1 Select Configuration → Devices → <device> → Edit:**



**2 Set the System Name to rfs6000-1 then assign the user defined RF Domain named noc and the Profile named noc-rfs6000. Click OK:**



3 Select *Profile Overrides* → *Interface* → *Virtual Interfaces*. If present select *vlan1* then click *Delete*. Click *Add* to create a new interface for the Native VLAN 20:

| Name  | Type | Description | Admin Status | VLAN | IP Address |
|-------|------|-------------|--------------|------|------------|
| vlan1 | VLAN |             | Enabled      | 1    | dhcp       |

4 Enter a *VLAN ID*, *Description* and *Primary IP Address* then click *OK*. Note that in this example the Cluster Masters IP address on VLAN 20 is *192.168.20.22/24*:

Virtual Interfaces

VLAN ID: 20 (1 - 4,094)

Basic Configuration | Security

Properties

Description: Management VLAN

Admin Status: Enabled

IP Addresses

Enable Zero Configuration:  None  Primary  Secondary

Primary IP Address: 192.168.20.22 / 24

Use DHCP to Obtain IP:

Use DHCP to obtain Gateway/DNS Servers:  (Allowed on 1 virtual interface)

Secondary Addresses: [Empty field]

DHCP Relay

Respond to DHCP Relay Packets:

DHCP Relay IP Address: [0.0.0.0 Clear] [0.0.0.0 Clear] [0.0.0.0 Clear] [0.0.0.0 Clear]

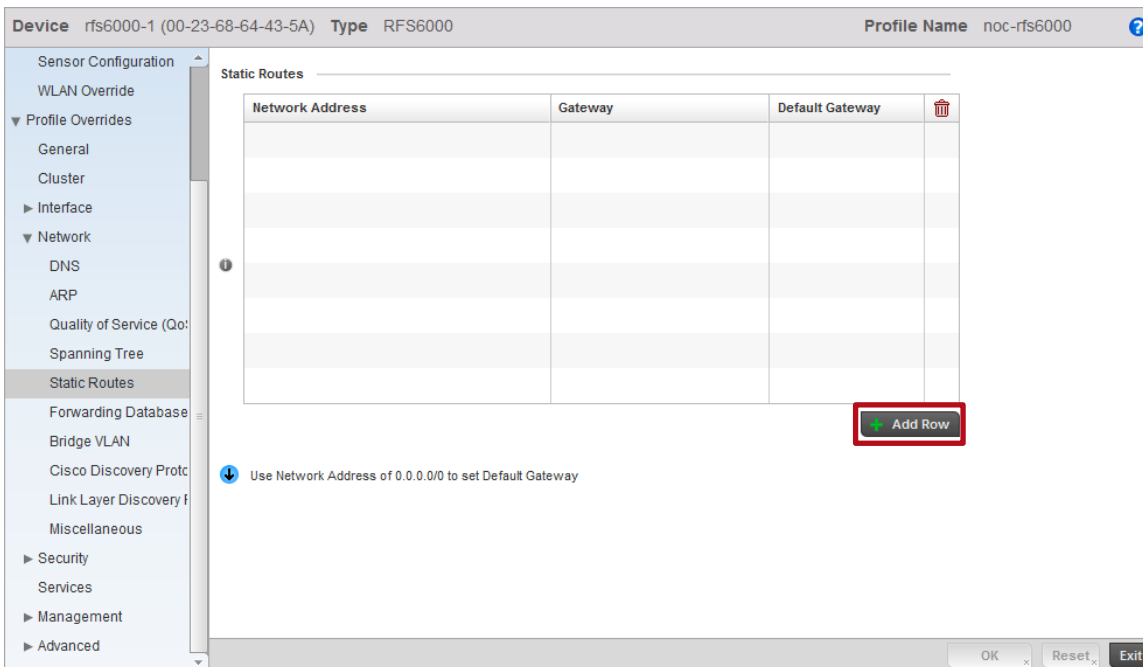
Network Address Translation (NAT)

NAT Direction:  Inside  Outside  None

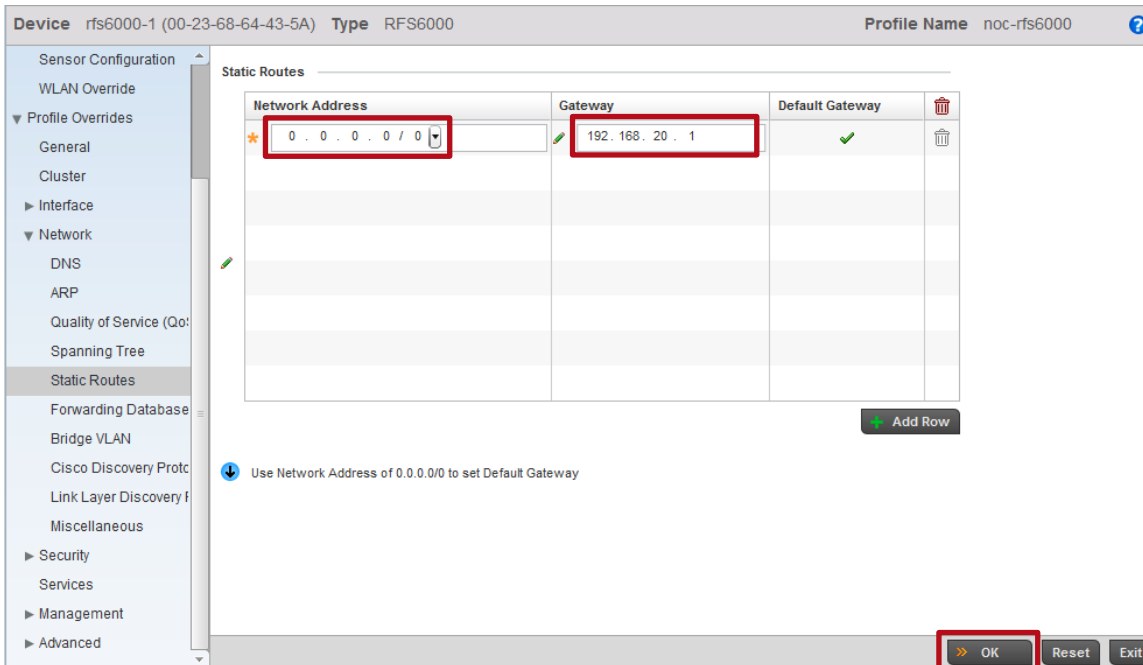
Buttons: OK, Reset, Exit



5 Select Profile Overrides → Network → Static Routes. Click Add Row:



6 In the Network Address field enter 0.0.0.0/0 then in the Gateway field enter the IP address of the default gateway. In this example 192.168.20.1 is the default gateway for VLAN 20. Click OK:



7 Select *Profile Overrides* → *Cluster*. In the *Cluster Name* field enter *noc* then set the *Master Priority* to *255*. Under *Cluster Member* click *Add Row*. Enter the *IP Address* assigned to the *Cluster Member* then set the *Routing Level* to *2*. Note that in this example the *Cluster Member* is assigned the static IP address *192.168.20.23*:

The screenshot shows the configuration page for a device (rfs6000-1) with profile name noc-rfs6000. The **Cluster Settings** section includes:
 

- Cluster Mode: Active (selected)
- Cluster Name: noc
- Master Priority: 255 (range 1 to 255)
- Handle STP Convergence: unchecked
- Force Configured State: unchecked
- Force Configured State Delay: 5 (range 3 to 1,800 minutes)

 The **Cluster Member** section includes:
 

- Cluster VLAN: 1 (range 1 to 4,094)
- Member IP Address: 192.168.20.23
- Routing Level: 2

 At the bottom, there are buttons for **Add Row**, **Restore Configured State**, **Force Active**, **Force Standby**, **OK**, **Reset**, and **Exit**.

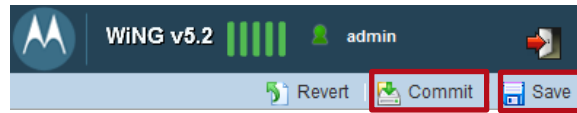
8 The Device configuration for the *Cluster Master* switch is now completed:

The screenshot shows the **Device Configuration** table with the following data:

| System Name | Device            | Type    | RF Domain Name | Profile Name | Area    | Floor   | Overrides |
|-------------|-------------------|---------|----------------|--------------|---------|---------|-----------|
| rfs6000-1   | 00-23-68-64-43-5A | RFS6000 | noc            | noc-rfs6000  | Not Set | Not Set | Clear     |

At the bottom of the table, there is a search input field labeled "Type to search in tables" and a "Row Count: 1" indicator. Action buttons for **Add**, **Edit**, and **Delete** are also present.

## 9 Commit then Save the changes:



## 2.5.2 Cluster Member Switch

For this configuration step the Wireless Controller that is designated as the Cluster Member will be assigned the following Device Configuration:

- 1) The default VLAN 1 will be removed (not applicable for the RFS7000 or NX9000).
- 2) The user defined **Profile** named **noc-rfs6000** will be assigned.
- 3) The user defined **RF Domain** named **noc** will be assigned.
- 4) The **Hostname** will be set to **rfs6000-2**.
- 5) A **Virtual IP Interface** for **VLAN 20** will be created and the IP address **192.168.20.23/24** assigned.
- 6) A default route pointing to **192.168.20.1** will be defined.
- 7) The cluster name will be set to **noc**.
- 8) The cluster priority will be set to **100** (lower than the Cluster Master).
- 9) A **Level 2 IP MINT Link** will be defined pointing to the Cluster Masters IP address **192.168.20.22**.



Note – Before adding the Cluster Members device configuration, the Cluster Members MAC address must be obtained. The Cluster Members MAC address can be obtained by logging into the Cluster Member and issuing the **show version command**.

### 2.5.2.1 Command Line Interface

Use the following procedure to modify the Device configuration for the Cluster Member using the Command Line Interface:

- 1 Using the obtained MAC address for the Cluster Member, create the Device configuration for the Cluster Member. In this example the Cluster Members MAC address is **5C-0E-8B-17-E8-F6**:

```
rfs6000-1(config)# rfs6000 5C-0E-8B-17-E8-F6
```

- 2 Assign the user defined RF Domain named **noc** and user defined Profile named **rfs6000-noc**:

```
rfs6000-1(config-device-5C-0E-8B-17-E8-F6)# use profile noc-rfs6000
```

```
rfs6000-1(config-device-5C-0E-8B-17-E8-F6)# use rf-domain noc
```

- 3 Define a **Hostname** for the device. Note in this example the hostname **rfs6000-2** is assigned:

```
rfs6000-1(config-device-5C-0E-8B-17-E8-F6)# hostname rfs6000-2
```

- 4 Create a *Virtual IP Interface* for the Native VLAN and assign a static IP address. Note in this example a Virtual IP interface for VLAN 20 has been created and the static IP address 192.168.20.23/24 assigned:**

```
rfs6000-1(config-device-5C-0E-8B-17-E8-F6) # interface vlan 20
rfs6000-1(config-device-5C-0E-8B-17-E8-F6-if-vlan20) # description Management
rfs6000-1(config-device-5C-0E-8B-17-E8-F6-if-vlan20) # ip address 192.168.20.23/24
rfs6000-1(config-device-5C-0E-8B-17-E8-F6-if-vlan20) # exit
```

- 5 Assign a default gateway. Note in this example the default gateway for VLAN 20 is 192.168.20.1:**

```
rfs6000-1(config-device-5C-0E-8B-17-E8-F6) # ip route 0.0.0.0/0 192.168.20.1
```

- 6 Define a *Cluster Name*, *Cluster Member IP Address* and set the *Cluster Priority* to 100. Note in this example the *Cluster Name* is set to *noc* and the *Cluster Members IP address* is 192.168.20.22. In addition the MINT link level between the cluster peers is set to *Level 2*:**

```
rfs6000-1(config-device-5C-0E-8B-17-E8-F6) # cluster name noc
rfs6000-1(config-device-5C-0E-8B-17-E8-F6) # cluster member ip 192.168.20.22 level 2
rfs6000-1(config-device-5C-0E-8B-17-E8-F6) # cluster master-priority 100
```

- 7 Verify the changes:**

```
rfs6000-1(config-device-5C-0E-8B-17-E8-F6) # show context

rfs6000 5C-0E-8B-17-E8-F6
use profile noc-rfs6000
use rf-domain noc
hostname rfs6000-2
ip default-gateway 192.168.20.1
interface vlan20
  description Management
  ip address 192.168.20.23/24
cluster name noc
cluster member ip 192.168.20.22 level 2
cluster master-priority 100
```

- 8 Exit the Profile configuration then *commit* and save the changes:**

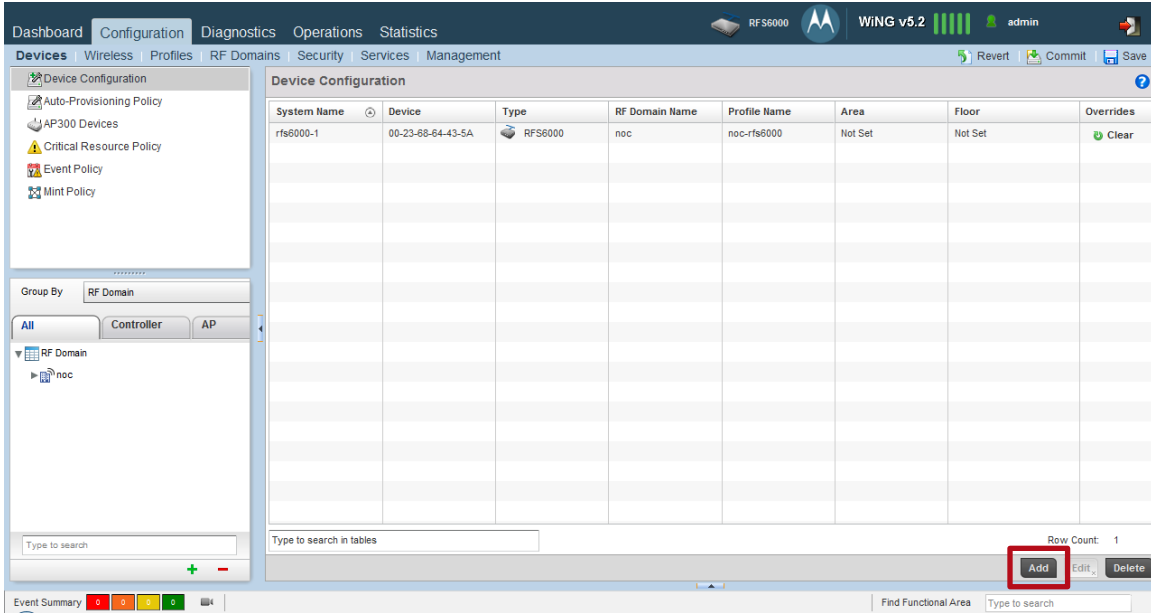
```
rfs6000-1(config-device-5C-0E-8B-17-E8-F6) # exit
rfs6000-1(config) # commit write
```

[OK]

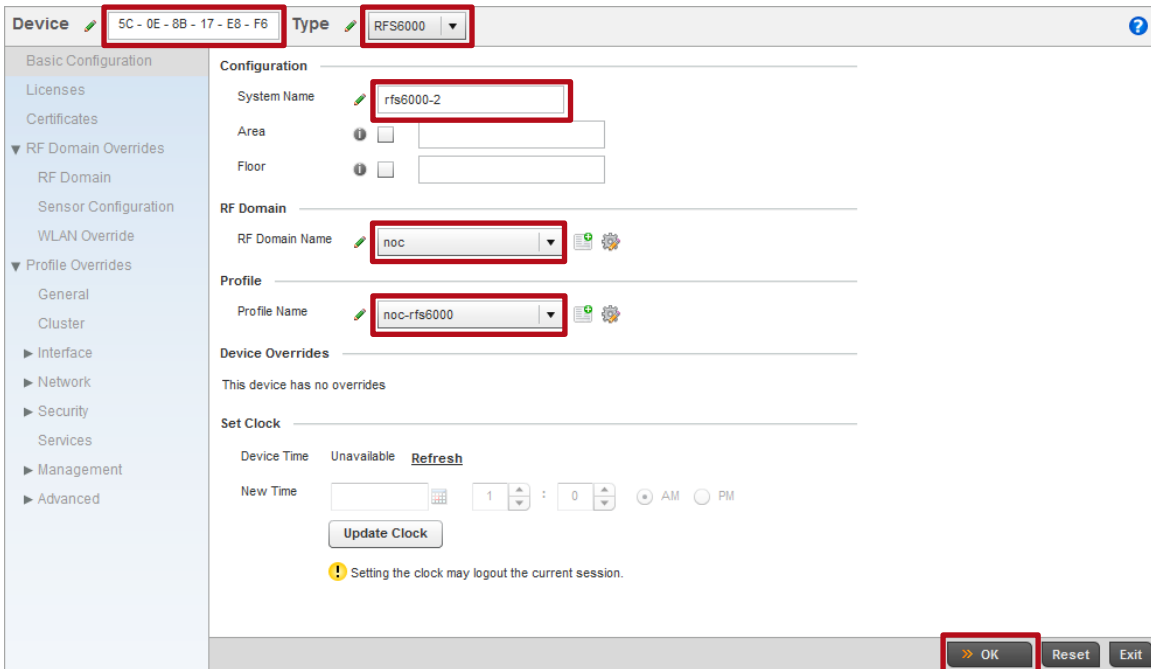
## 2.5.2.2 Management User Interface

Use the following procedure to modify the Device configuration for the Cluster Member using the Management User Interface:

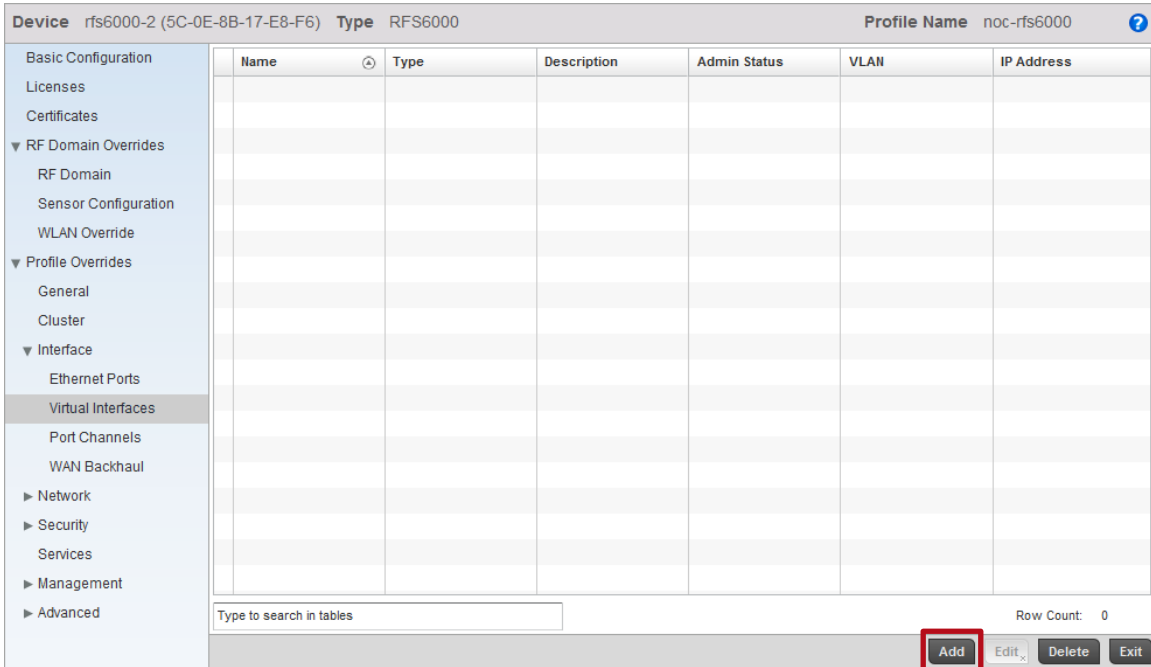
### 1 Select Configuration → Devices → Add:



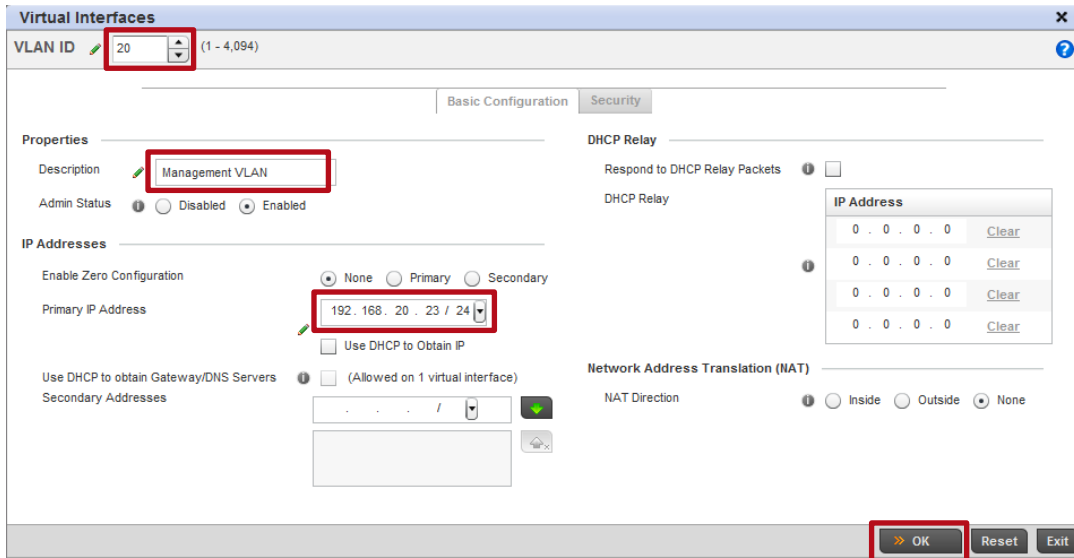
### 2 Enter the Cluster Members Device MAC address and set the Type to RFS6000. Set the System Name to rfs6000-2 then assign the user defined RF Domain named noc and the Profile named noc-rfs6000. Click OK:



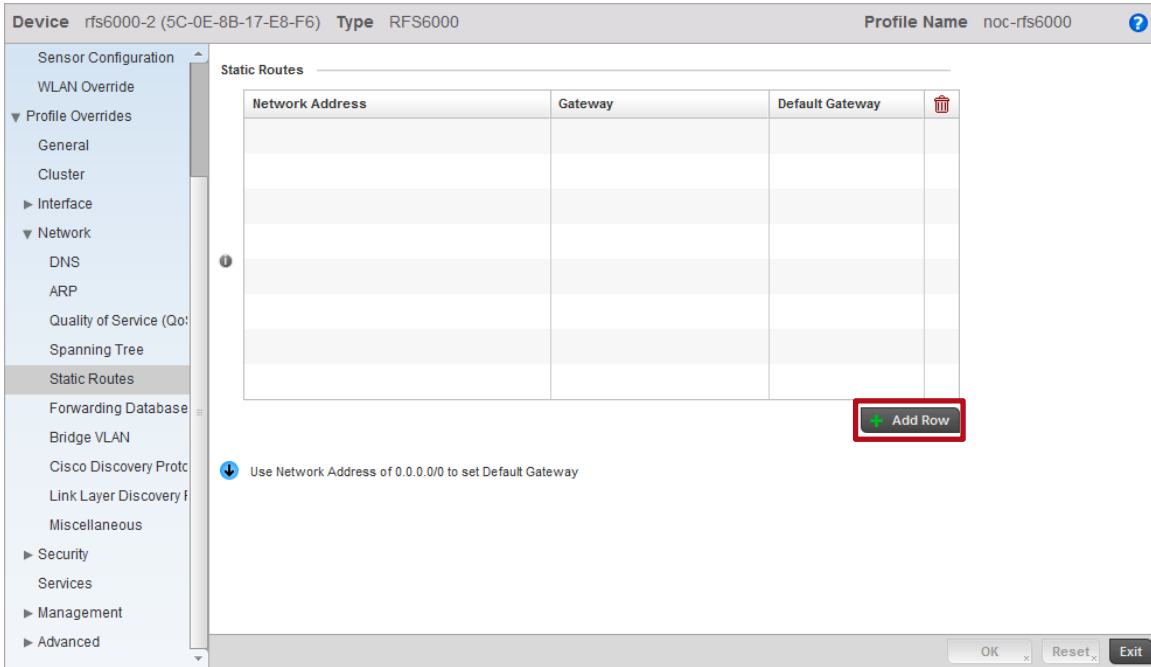
3 Select Profile Overrides → Interface → Virtual Interfaces → Add:



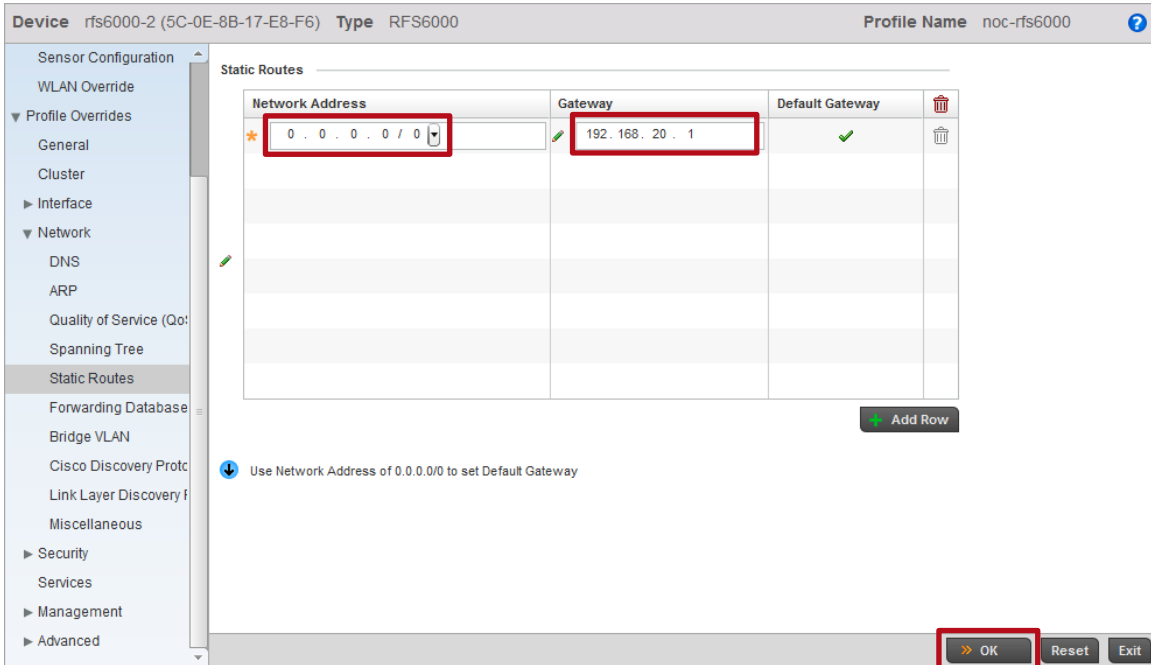
4 Enter a VLAN ID, Description and Primary IP Address then click OK. Note that in this example the Cluster Members IP address on VLAN 20 is 192.168.20.23/24:



5 Select Profile Overrides → Network → Static Routes. Click Add Row:



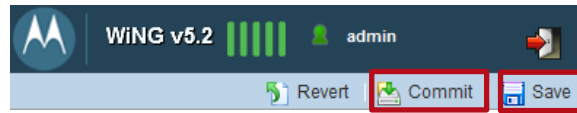
6 In the Network Address field enter 0.0.0.0/0 then in the Gateway field enter the IP address of the default gateway. In this example 192.168.20.1 is the default gateway for VLAN 20. Click OK:







## 9 Commit then Save the changes:



## 2.6 Automatic Provisioning Policies

By default WiNG 5.X devices are assigned to a default RF Domain and device Profile based on their model type. Automatic Provisioning Policies provide a mechanism that allows the Wireless Controllers in the data center / NOC to automatically assign a user defined Profile and RF Domain to remote Access Points as they are initially discovered and adopted by a Wireless Controller. Without Automatic Provisioning Policies an administrator would have to manually assign the correct user defined Profile and RF Domain to each individual Access Point.

Automatic Provisioning Policies contain one or more rules for each model of Access Point with match conditions and values that assigns the correct user defined Profile and RF Domain during initial adoption. For data center / NOC deployments these rules are typically based on the IP subnet the Access Points are connected too, however matches can also be made based on other values such as a location provided by CDP or LLDP advertisements from the Ethernet infrastructure deployed at the remote site.

For this configuration step an Automatic Provisioning Policy with two rules will be created with the following parameters:

- 1) An Automatic Provisioning Policy named **noc** will be created and assigned to the RFS6000 user defined Profile named **rfs6000-noc**.
  - a. An AP6532 rule for store 100 assigning the user defined **RF Domain** named **store100** and user defined Profile named **ap6532-stores** will be defined with a match based on the source subnet **192.168.21.0/24**.
  - b. An AP6532 rule for store 101 assigning the user defined **RF Domain** named **store101** and user defined Profile named **ap6532-stores** will be defined with a match based on the source subnet **192.168.31.0/24**.



Note – At least one Automatic Provisioning Policy rule will be required for each remote site. As rules are Access Point model dependent, multiple rules may be required if multiple Access Point models are deployed. For example if both AP7131 and AP6532 Access Points are deployed at a site, two Automatic Provisioning Policy rules will be required for that site.

## 2.6.1 Command Line Interface

Use the following procedure to create and assign Automatic Provisioning Policy and rules using the Command Line Interface:

- 1 Create an Automatic Provisioning Policy named *noc* with rules. In this example two rules will be defined for AP6532 Access Points that assigns the user defined Profile named *stores-ap6532* and RF Domain *store100* or *store101* based on the IP subnet the AP6532 Access Points are connected to:

```
rfs6000-1(config)# auto-provisioning-policy noc
rfs6000-1(config-auto-provisioning-policy-noc)# adopt ap6532 precedence 1 profile stores-ap6532 rf-domain store100 ip 192.168.21.0/24
rfs6000-1(config-auto-provisioning-policy-noc)# adopt ap6532 precedence 2 profile stores-ap6532 rf-domain store101 ip 192.168.31.0/24
```

- 2 Verify the changes:

```
rfs6000-1(config-auto-provisioning-policy-noc)# show context
auto-provisioning-policy noc
adopt ap6532 precedence 1 profile stores-ap6532 rf-domain store100 ip 192.168.21.0/24
adopt ap6532 precedence 2 profile stores-ap6532 rf-domain store101 ip 192.168.31.0/24
```

- 3 Exit the Automatic Provisioning Policy configuration:

```
rfs6000-1(config-auto-provisioning-policy-noc)# exit
```

- 4 Access the RFS6000 user defined Profile named *noc-rfs6000* and assign the Automatic Provisioning Policy named *noc*:

```
rfs6000-1(config)# profile rfs6000 noc-rfs6000
rfs6000-1(config-profile-noc-rfs6000)# use auto-provisioning-policy noc
```

- 5 Verify the changes:

```
rfs6000-1(config-profile-noc-rfs6000)# show context
profile rfs6000 noc-rfs6000
ip name-server 192.168.10.5
ip domain-name tmlabs.local
!
! Unnecessary configuration omitted for brevity
!
use management-policy noc
use firewall-policy default
use auto-provisioning-policy noc
ntp server 192.168.10.5
service pm sys-restart
```

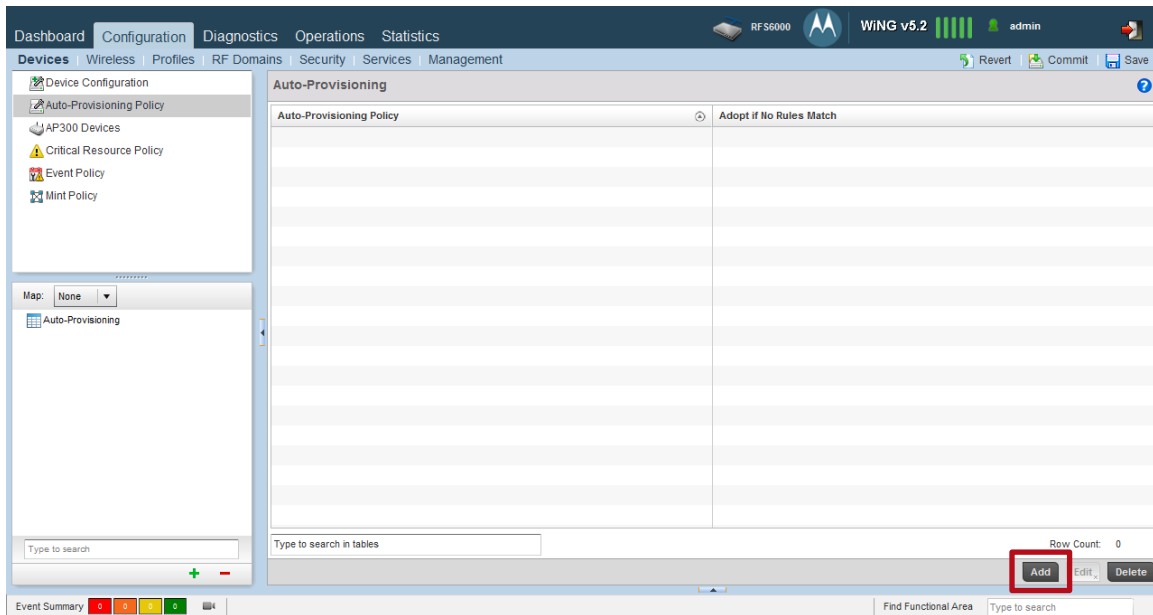
**6 Exit the Profile configuration then *commit* and save the changes:**

```
rfs6000-1 (config-profile-noc-rfs6000) # exit
```

```
rfs6000-1 (config) # commit write
```

## 2.6.2 Management User Interface

Use the following procedure to create and assign Automatic Provisioning Policy and rules using the Management User Interface:

**1 Select *Configuration* → *Devices* → *Auto-Provisioning Policy* → *Add*:**

2 Enter the Auto-Provisioning Policy name noc then click Continue:

The screenshot shows the 'Auto-Provisioning Policy' configuration interface. At the top, there is a header bar with the text 'Auto-Provisioning Policy' and a search icon. Below this, a text input field contains the value 'noc'. To the right of the input field are two buttons: 'Continue' and 'Exit'. The 'Continue' button is highlighted with a red rectangular box. Below the header is a tabbed interface with 'Rules' and 'Default' tabs. The 'Default' tab is active, showing a table with the following columns: 'Rule Precedence', 'Allow', 'Device Type', 'Match Type', 'Argument 1', 'Argument 2', 'RF Domain Name', and 'Profile Name'. The table is currently empty. At the bottom of the interface, there is a search bar with the placeholder text 'Type to search in tables' and a 'Row Count: 0' indicator. On the far right, there are four buttons: 'Add', 'Edit', 'Delete', and 'Exit'.

3 Click Add:

This screenshot shows the same 'Auto-Provisioning Policy' configuration page as above, but now the policy name 'noc' is visible in the top header. The 'Add' button at the bottom right of the interface is highlighted with a red rectangular box. The rest of the page, including the table and search bar, remains the same as in the previous screenshot.

- 4 Set the *Rule Precedence* to 1 then set the *Device Type* to AP6532. Set the *Match Type* to IP Address then enter the IP Subnet the Access Points are connected to at the first site (example 192.168.21.0/24). Assign the *RF Domain* named store100 and the *Profile* named stores-ap6532. Click OK then Exit:

The screenshot shows the 'Rule' configuration window with the following details:

- Rule Precedence:** 1 (range 1 to 10,000)
- Auto-Provisioning Policy:** Allow
- Device:** Device Type: AP6532 (selected)
- Match Parameters:** Match Type: IP Address; Subnet: 192.168.21.0 / 24
- Map to Profile / RF Domain:** RF Domain Name: store100; Profile Name: stores-ap6532
- Buttons:** OK, Reset, Exit

- 5 Click Add. Set the *Rule Precedence* to 2 then set the *Device Type* to AP6532. Set the *Match Type* to IP Address then enter the IP Subnet the Access Points are connected to at the second site (example 192.168.31.0/24). Assign the *RF Domain* named store101 and the *Profile* named stores-ap6532. Click OK then Exit:

The screenshot shows the 'Rule' configuration window with the following details:

- Rule Precedence:** 2 (range 1 to 10,000)
- Auto-Provisioning Policy:** Allow
- Device:** Device Type: AP6532 (selected)
- Match Parameters:** Match Type: IP Address; Subnet: 192.168.31.0 / 24
- Map to Profile / RF Domain:** RF Domain Name: store101; Profile Name: stores-ap6532
- Buttons:** OK, Reset, Exit

6 An Automatic Provisioning Policy with two rules has now been defined. Click *Exit*:

Auto-Provisioning Policy noc

| Rule Precedence | Allow | Device Type | Match Type | Argument 1      | Argument 2 | RF Domain Name | Profile Name  |
|-----------------|-------|-------------|------------|-----------------|------------|----------------|---------------|
| 1               | ✓     | AP6532      | IP Address | 192.168.21.0/24 |            | store100       | stores-ap6532 |
| 2               | ✓     | AP6532      | IP Address | 192.168.31.0/24 |            | store101       | stores-ap6532 |

Type to search in tables

Row Count: 2

Add Edit Delete **Exit**

7 Commit the changes:

WING v5.2 admin

Revert **Commit** Save

8 Select Configuration → Profiles → noc-rfs6000 → Edit:

Dashboard Configuration Diagnostics Operations Statistics RFS6000 WING v5.2 admin

Devices Wireless Profiles RF Domains Security Services Management

Manage Profiles

| Profile        | Type    | Auto-Provisioning Policy | Firewall Policy | Wireless Client Role Policy | Advanced WIPS Policy | DHCP Server Policy | Management Policy | RADIUS Server Policy |
|----------------|---------|--------------------------|-----------------|-----------------------------|----------------------|--------------------|-------------------|----------------------|
| default-ap621  | AP621   |                          | default         |                             |                      |                    | default           |                      |
| default-ap650  | AP650   |                          | default         |                             |                      |                    | default           |                      |
| default-ap6511 | AP6511  |                          | default         |                             |                      |                    | default           |                      |
| default-ap6521 | AP6521  |                          | default         |                             |                      |                    | default           |                      |
| default-ap6532 | AP6532  |                          | default         |                             |                      |                    | default           |                      |
| default-ap71xx | AP71XX  |                          | default         |                             |                      |                    | default           |                      |
| noc-rfs6000    | RFS6000 |                          | default         |                             |                      |                    | noc               |                      |
| stores-ap6532  | AP6532  |                          | default         |                             |                      |                    | stores            |                      |

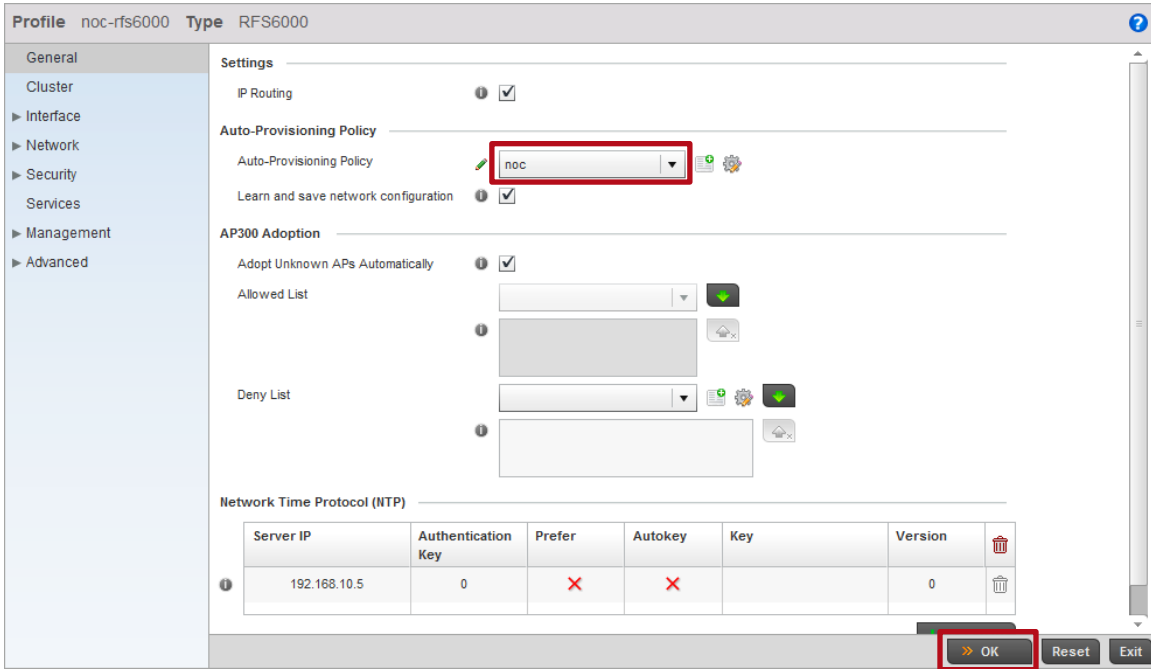
Type to search

Type to search in tables

Row Count: 9

Add Edit **Edit** Delete

9 Select *General* then assign the *Auto-Provisioning Policy* named *noc*. Click *OK* then *Exit*:

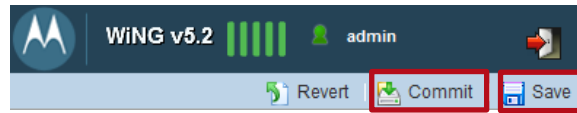


10 The Automatic Provisioning Policy named *noc* has now been assigned to the RFS6000 user defined Profile named *noc-rfs6000*:

| Profile         | Type    | Auto-Provisioning Policy | Firewall Policy | Wireless Client Role Policy | Advanced WIPS Policy | DHCP Server Policy | Management Policy | RADIUS Server Policy |
|-----------------|---------|--------------------------|-----------------|-----------------------------|----------------------|--------------------|-------------------|----------------------|
| default-ap621   | AP621   |                          | default         |                             |                      |                    | default           |                      |
| default-ap650   | AP650   |                          | default         |                             |                      |                    | default           |                      |
| default-ap6511  | AP6511  |                          | default         |                             |                      |                    | default           |                      |
| default-ap6521  | AP6521  |                          | default         |                             |                      |                    | default           |                      |
| default-ap6532  | AP6532  |                          | default         |                             |                      |                    | default           |                      |
| default-ap71xx  | AP71XX  |                          | default         |                             |                      |                    | default           |                      |
| default-rfs6000 | RFS6000 |                          | default         |                             |                      |                    | default           |                      |
| noc-rfs6000     | RFS6000 | noc                      | default         |                             |                      |                    | noc               |                      |
| stores-ap6532   | AP6532  |                          | default         |                             |                      |                    | stores            |                      |

The table shows a list of profiles. The row for 'noc-rfs6000' is highlighted with a red box, indicating that the 'Auto-Provisioning Policy' is now set to 'noc'. The 'Management Policy' is also set to 'noc'. At the bottom right of the table, there are buttons for 'Add', 'Edit', and 'Delete', and a 'Row Count: 9' indicator.

## 11 Commit then Save the changes:



## 2.7 Forming the Cluster

Now that the Wireless Controller configuration is complete, we can now copy the configuration created on the Cluster Master controller to the Cluster Member controller. Once the configuration has been copied and the Cluster Member switch reset, the RFS6000s in the cluster will establish MINT links, elect a master then become active. The configuration on the master controller will be automatically synchronized on the cluster member.

### 2.7.1 Command Line Interface

Use the following procedure to modify the Device configuration for the Cluster Master switch using the Command Line Interface:

#### 1 On the Cluster Master switch copy the running-config to a USB key:

```
rfs6000-1# copy running-config usb1:cluster.cfg
```

#### 2 Move the USB key to the Cluster Member switch then copy the configuration file to the Cluster Members switches startup-config:

```
rfs6000-17E8F6# copy usb1:cluster.cfg startup-config
```

#### 3 Reload the Cluster Member controller:

```
rfs6000-17E8F6# reload
```

The system will be rebooted, do you want to continue? (y/n): **y**

Save current configuration? ([y]es/[n]o/[d]isplay unsaved/[c]ancel reload): **n**

#### 4 Once the Cluster Member switch has initialized the Cluster will go through an election process and elect a *Cluster Master*. The configuration will synchronize and the Cluster will become operational. In this example *rfs6000-1* with the priority 255 has become the *Cluster Master* and *rfs6000-2* with the priority 100 has become a *Cluster Member*.

```
rfs6000-1# show cluster members
```

Cluster master election in progress

Configured cluster members

00-23-68-64-43-5A

5C-0E-8B-17-E8-F6

| HOSTNAME  | MEMBER-ID   | MAC               | MASTER       | STATE  | STATUS | LAST-SEEN    |
|-----------|-------------|-------------------|--------------|--------|--------|--------------|
| rfs6000-1 | 68.64.43.5A | 00-23-68-64-43-5A | <b>True</b>  | active | up     | 00:00:12 ago |
| rfs6000-2 | 0B.17.E8.F6 | 5C-0E-8B-17-E8-F6 | <b>False</b> | active | up     | 00:00:10 ago |



**5 Use the *show cluster member detail* command to display additional information such as each Wireless Controllers AP and AAP license counts:**

```
rfs6000-1# show cluster members detail
```

| ID          | MAC               | MODE   | AP COUNT | AAP COUNT | AP LICENSE | AAP LICENSE | VERSION      |
|-------------|-------------------|--------|----------|-----------|------------|-------------|--------------|
| 68.64.43.5A | 00-23-68-64-43-5A | Active | 0        | 0         | 48         | 256         | 5.2.0.0-061R |
| 0B.17.E8.F6 | 5C-0E-8B-17-E8-F6 | Active | 0        | 0         | 0          | 0           | 5.2.0.0-061R |

**6 Use the *show cluster status* command to display Cluster Runtime Information. This will display the overall *Cluster State, License Pooling* and *Adoption Capacity* information:**

```
rfs6000-1# show cluster status
```

Cluster Runtime Information

```
Protocol version      : 1
Cluster state        : active
AP license           : 48
AAP license          : 256
AP count             : 0
AAP count            : 0
Max AP adoption capacity : 512
Number of connected member(s): 1
```

## 2.8 DHCP Services

To support remote plug-n-play Access Point deployments, the Access Points at each remote site will require DHCP services on their Native VLAN for network addressing as well as Motorola DHCP option 191 parameters and values to discover the Wireless Controllers located in the data center / NOC. The DHCP deployment maybe centralized using DHCP services located in the data center / NOC or distributed using DHCP services deployed locally at each site.

In a NOC deployment model the remote Access Points use Motorola DHCP option 191 to form Level 2 IP based MINT links to the Wireless Controllers in the data center / NOC. The Motorola Option 191 parameters and values provide remote Access Points with the IP Addresses and/or Hostnames of the Wireless Controllers along with the MINT level the Access Points should utilize to communicate with the Wireless Controllers. The option 191 parameters and value can also be utilized to assign advanced parameters such as the UDP port used for MiNT encapsulation in addition to timers.

The following table provides some example standard Motorola DHCP option 191 values which can be utilized for most NOC based deployments:

### Standard DHCP Option 191 Values:

```
pool1=192.168.20.22,192.168.20.23;level=2
```

```
pool1=rfs6000-1.tmelabs.local;rfs6000-2.tmelabs.local;level=2
```

```
pool1=192.168.20.22;rfs6000-2.tmelabs.local;level=2
```

**Table 2.8 – Standard DHCP Option 191 Parameters & Values Examples**

### 2.8.1 Advanced DHCP Option 191 Parameters

WiNG 5.2.1 and above introduces three new Motorola DHCP option 191 parameters which can be enabled to address challenges in more advanced deployments. The advanced parameters and values can be utilized to provide remote Access Points with the UDP port used for MiNT encapsulation in addition to the timers used to exchange MiNT hello packets and how long the Controller waits between hello intervals before determining a remote Access Point is offline:

- **udp-port** – Defines the UDP port used for MiNT encapsulation over IP (default 24576).
- **hello-interval** – Defines the interval between MiNT hello packets exchanged between the NOC Controllers and Access Points (default 15).
- **adjacency-hold-time** – Defines the maximum period since the last MiNT hello packet was received before the MiNT link is considered down (default 45).

The `udp-port` parameter must be supplied to the remote Access Points if the default UDP port in the MiNT policy assigned on the NOC Controllers has been modified. By default the NOC Controllers and remote Access Points will utilize UDP port 24576 which is defined in the global MiNT policy named `global-mint` that is assigned to all devices. If the default UDP port is modified, the new DHCP option 191 parameter must be provided to the remote Access Points so that they know how to communicate with the centralized NOC controllers. Failure to provide the UDP port with the DHCP option will result in adoption failures.

The `hello-interval` and `adjacency-hold-time` parameters determine the interval between MiNT hello packets exchanged between the NOC Controllers and Access Points in addition to the time interval each device waits when no MiNT hello packets are received before determining the MiNT link is down. By default for IP based MiNT links the `hello-interval` is 15 seconds and the `adjacency-hold-time` is 45.

Increasing the default hello-interval and adjacency-hold-time parameters may be necessary in certain high-latency or oversubscribed WAN deployments to ensure that Access Points at remote sites stay on-line and are not marked as offline when default MiNT timers are exceeded.

When increasing the hello-interval and adjacency-hold-time parameters it is a best practice recommendation that the hello-interval value be set to 1/3<sup>rd</sup> the adjacency-hold-time value. For example if the adjacency-hold-time value is set to 60 seconds, the hello-interval must be set to 20 seconds. The adjacency-hold-time should always be one or two seconds more than the hello-interval to maintain the MiNT link.

#### Advanced DHCP Option 191 Values:

```
pool1=192.168.20.22,192.168.20.23;udp-port=031102;level=2
```

```
pool1=rfs6000-1.tmelabs.local;rfs6000-2.tmelabs.local;level=2;hello-interval=20;adjacency-hold-time=60
```

**Table 2.8.1 – Advanced DHCP Option 191 Parameters & Values Examples**



Note – Any **hello-interval** and **adjacency-hold-time** values assigned from DHCP option 191 will supersede any values assigned to a Profile or directly to a device as override.

## 2.8.2 Option 60 Vendor Class

As DHCP option 191 maybe used by other networked devices within the Access Points Native VLAN, Motorola WiNG 5.X Access Point supports a unique Vendor Class Identifier which is based on the Access Point model. The Vendor Class Identifier is provided to the DHCP server with the DHCP Discover and DHCP ACK messages.

DHCP administrators can configure the DHCP server to use the provided Vendor Class Identifiers to only assign vendor specific options to the Motorola Access Points and not to all devices within the DHCP scope. Some DHCP servers also provide the ability to assign these options globally eliminating the need for assigning Motorola option 191 to multiple individual DHCP scopes.

The following table provides the Vendor Class Identifiers for each of the WiNG 5.X supported Motorola Access Points:

| Access Point | Vendor Class Identifier |
|--------------|-------------------------|
| AP621        | MotorolaAP.AP621        |
| AP650        | MotorolaAP.AP650        |
| AP6511       | MotorolaAP.AP6511       |
| AP6521       | MotorolaAP.AP6521       |
| AP6532       | MotorolaAP.AP6532       |
| AP7131       | MotorolaAP.AP7131       |

**Table 2.8.2 – Motorola Vendor Class Identifiers**

## 2.8.3 DHCP Server Implementation Examples

### 2.8.3.1 Cisco IOS Based DHCP Server

Cisco IOS based devices such as Routers and certain Catalyst Switches provide support for integrated DHCP services. An IOS based device at a remote store can be utilized to provide local DHCP services for the site. When an IOS based DHCP server is utilized at a store, the Motorola option 191 value must be assigned directly to the DHCP scope providing DHCP services to the Access Points Native VLAN at the store.

Use the following procedure to create a DHCP scope on a Cisco IOS based DHCP server that will assign Motorola DHCP option 191 and values from within the scope:

- 1 For the DHCP scope supporting the Access Points Native VLAN at the site, create a range of excluded addresses:**

```
C3725-1 (config) # ip dhcp excluded-address 192.168.21.1 192.168.21.99
```

- 2 Create a DHCP pool for the Access Points Native VLAN and define the required parameters and standard options:**

```
C3725-1 (config) # ip dhcp pool MotorolaAPs
C3725-1 (dhcp-config) # import all
C3725-1 (dhcp-config) # network 192.168.21.0 255.255.255.0
C3725-1 (dhcp-config) # domain-name tmelabs.local
C3725-1 (dhcp-config) # dns-server 192.168.10.5
C3725-1 (dhcp-config) # default-router 192.168.21.1
```

- 3 Define Motorola option 191 as an ASCII string. In this example the Access Points will be provided the Wireless Controller IP addresses 192.168.20.22 and 192.168.20.23 and will establish Level 2 IP based MINT links to the Wireless Controllers:**

```
C3725-1 (dhcp-config) # option 191 ascii pool1=192.168.20.22,192.168.20.23;level=2
```

- 4 Exit the DHCP pool then apply the changes:**

```
C3725-1 (dhcp-config) # end
C3725-1# write memory
```

### 2.8.3.2 Linux ISC DHCP Server

Most Linux distributions provide support for the ISC DHCP server may be deployed centrally in the data center / NOC or locally at each store. The Microsoft DHCP server supports the ability to assign Motorola option 191 values directly to each DHCP scope as well as globally across multiple scopes using the Vendor Class Identifier.

Use the following procedure to modify the ***dhcpd.conf*** configuration file and define an Option Code, Vendor Class and DHCP Scope. The Linux ISC DHCP server that will globally assign Motorola DHCP option 191 and values to Access Points across multiple DHCP scopes:

#### 1 Define DHCP option code 191 as a *String*:

```
# option Code for wireless controller Discovery
option ControllerIPAddress code 191 = string;
```

#### 2 Define the *Class* for each model of Access Point and assign option 191. In this example a Vendor Class Identifier for an AP6532 has been defined. AP6532 Access Points will be provided with the Wireless Controller IP addresses 192.168.20.22 and 192.168.20.23 and will establish Level 2 IP based MINT links to the Wireless Controllers:


```
# Vendor Class for Motorola AP6532 Access Points
class "MotorolaAP.AP6532" {
    match if substring(option vendor-class-identifier, 0, 17) = "MotorolaAP.AP6532";
    option vendor-class-identifier "MotorolaAP.AP6532";
    option ControllerIPAddress "pool1=192.168.20.22,192.168.20.23;level=2";
}
```

#### 3 Create a DHCP scope for the Access Points Native VLAN and define the required parameters and standard options:

```
# DHCP Scope for the Access Points Native VLAN
subnet 192.168.21.0 netmask 255.255.255.0 {
    range 192.168.21.100 192.168.21.254;
    default-lease-time 86400;
    max-lease-time 86400;
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.21.255;
    option routers 192.168.21.1;
    option domain-name tmlabs.local;
    option domain-name-server 192.168.10.5;
}
```

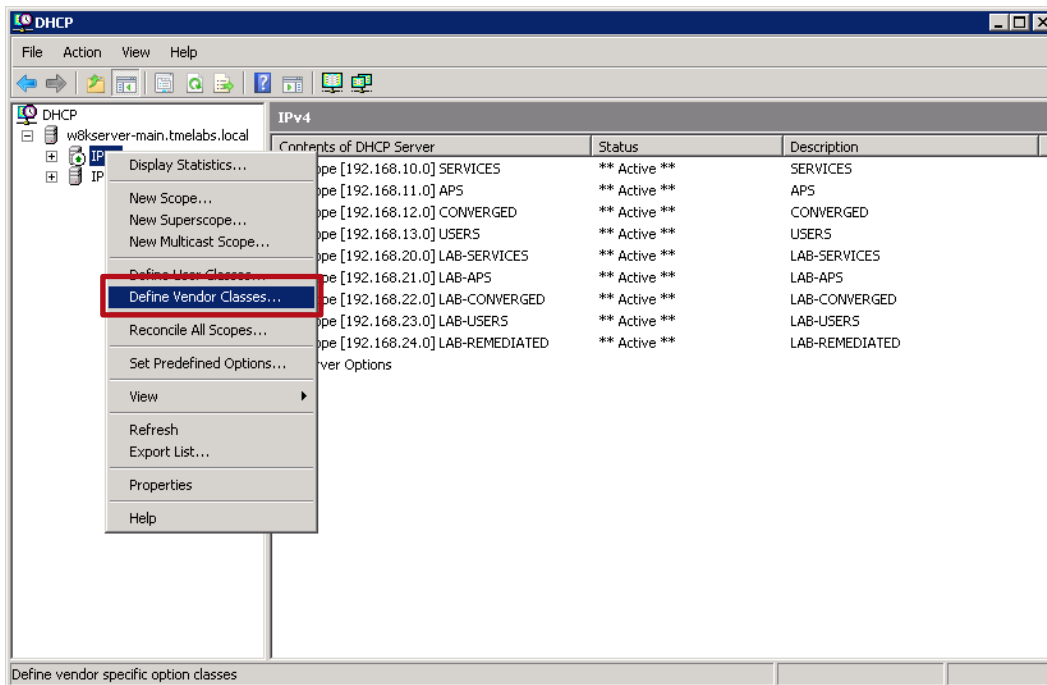
### 2.8.3.3 Microsoft Windows DHCP Server

Microsoft Windows Server 2003 and 2008 provide integrated DHCP services which may be deployed centrally in the data center / NOC or locally at each store. The Microsoft DHCP server supports the ability to assign Motorola option 191 values directly to each DHCP scope as well as globally across multiple scopes using the Vendor Class Identifier. When a Microsoft based DHCP server is utilized, the Motorola option 191 value must be assigned directly to each DHCP scope providing DHCP services to the Access Points Native VLAN.

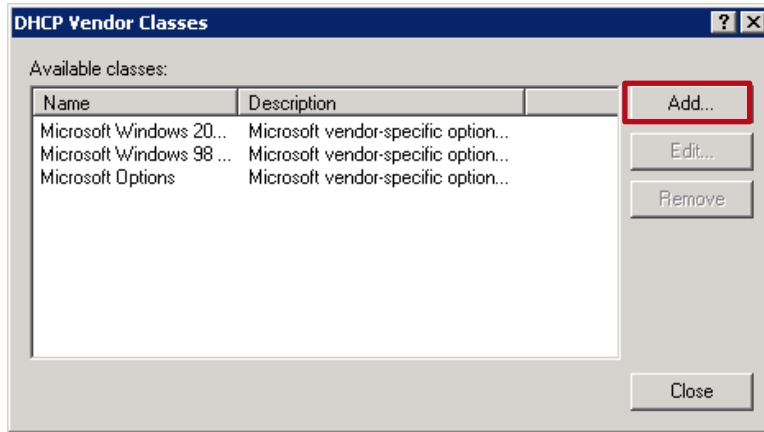
 Note – Please reference the relevant Microsoft documentation for assigning DHCP options globally across multiple scopes as this procedure varies by Windows Server version.

Use the following procedure to create a Vendor Class Identifier and Predefined options 191 values on a Microsoft DHCP server that will assign Motorola DHCP option 191 and values from a specific DHCP scope:

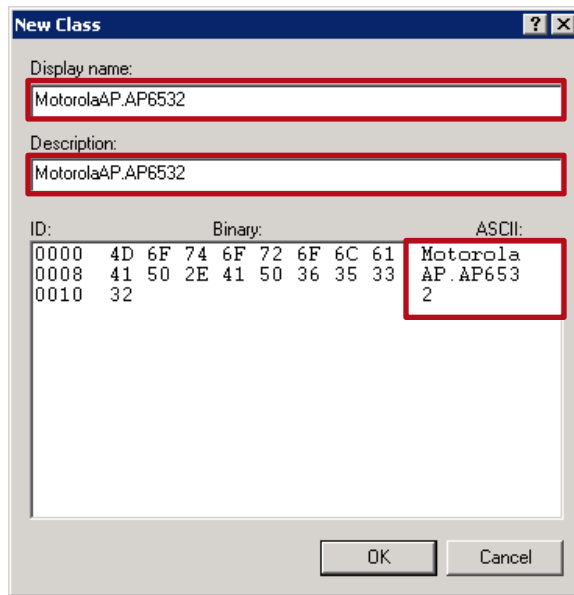
1 In the DHCP snap-in, right click on the *DHCP Server* icon then select *Define Vendor Classes*:



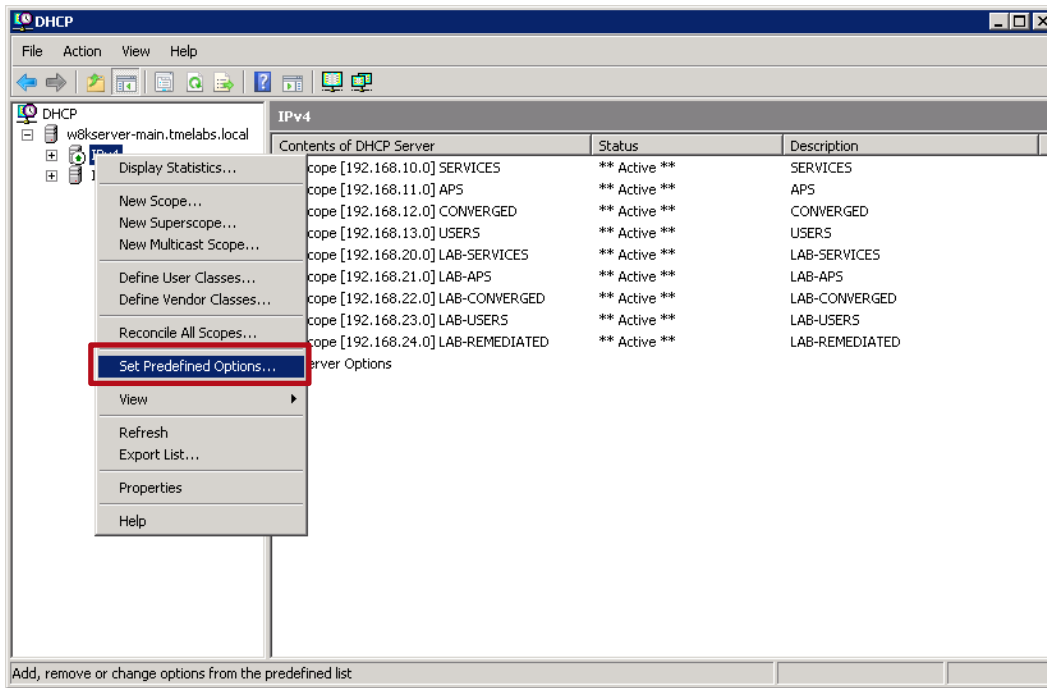
2 Click *Add*:



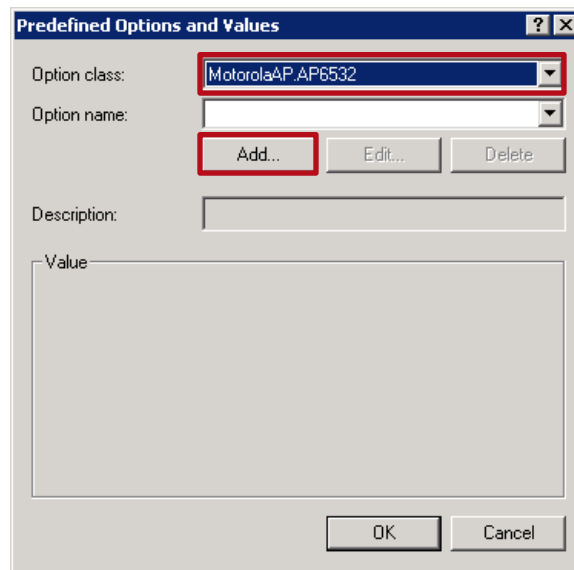
3 Enter the *Display Name* and *Description*. In the *ASCII* field type the *Vendor Class Identifier* for the Access Point model then click *OK*. Note in this example the Vendor Class for the AP6532 Access Points *MotorolaAP.AP6532* is defined:



- 4 In the DHCP snap-in, right click on the *DHCP Server* icon then select *Set Predefined Options*:



- 5 Select the *Option class* name created earlier then click *Add*:





- 6 Enter a *Name* and *Description* for the option then set the *Data type* to *String*. In the *Code* field enter 191 then click *OK*:

The 'Option Type' dialog box shows the following configuration:

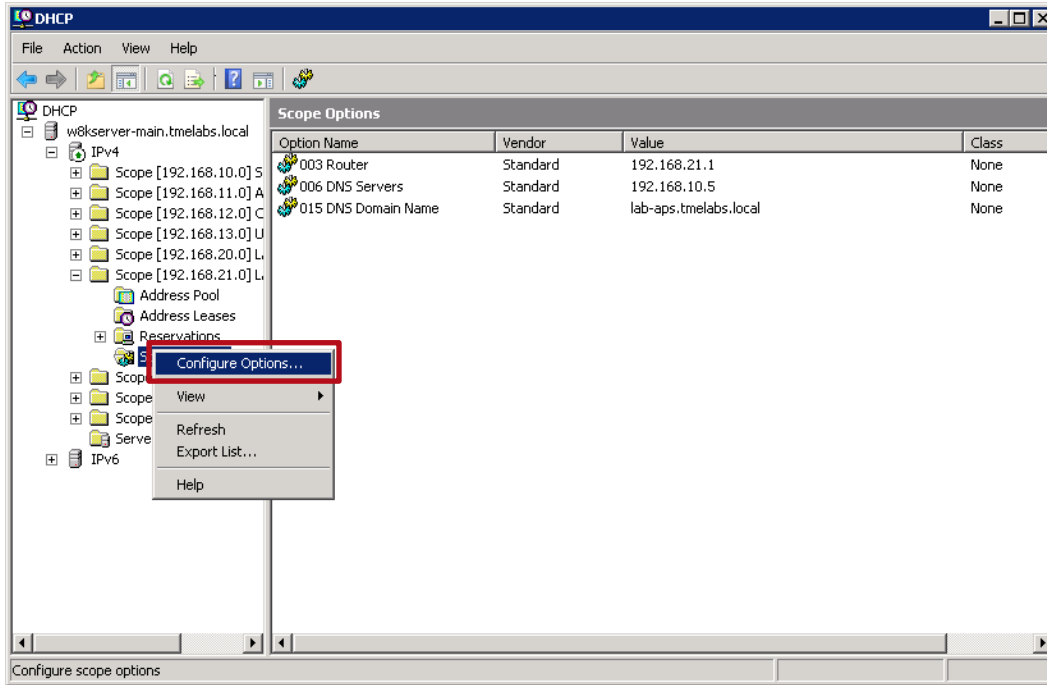
- Class: MotorolaAP.AP6532
- Name: ControllerIPAddress
- Data type: String (with an unchecked Array checkbox)
- Code: 191
- Description: ControllerIPAddress

- 7 In the *String* field enter the value to provide to the Motorola Access Points. In this example AP6532 Access Points will be provided the Wireless Controller IP addresses 192.168.20.22 and 192.168.20.23 and will establish *Level 2* IP based MINT links to the Wireless Controllers. Click *OK*:

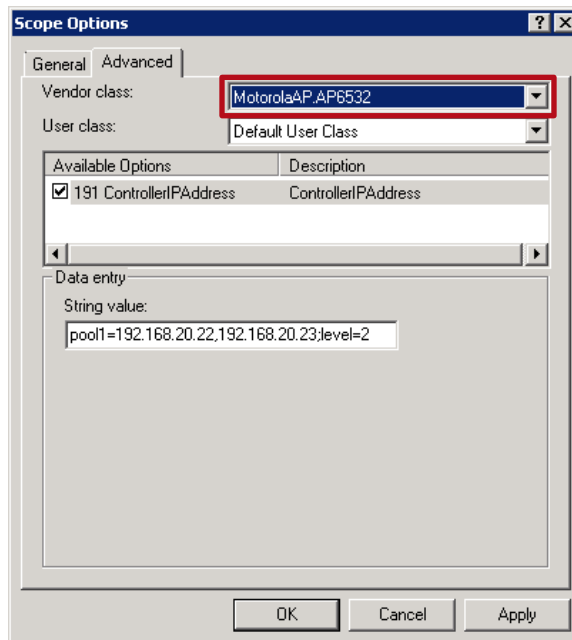
The 'Predefined Options and Values' dialog box shows the following configuration:

- Option class: MotorolaAP.AP6532
- Option name: 191 ControllerIPAddress
- Description: ControllerIPAddress
- Value (String): pool1=192.168.20.22,192.168.20.23;level=2

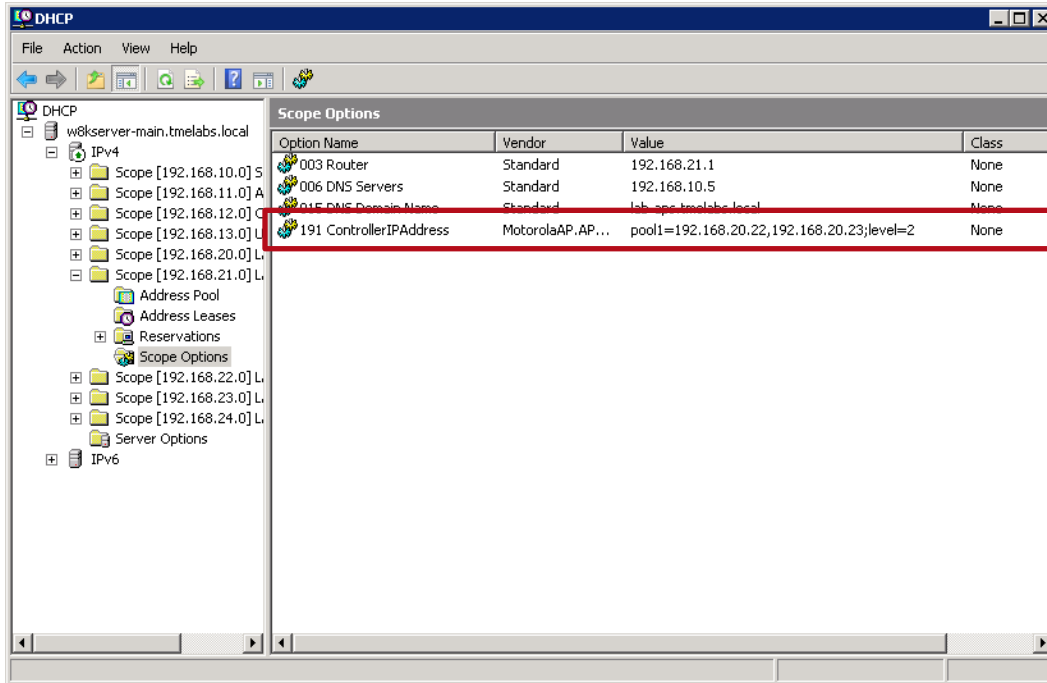
- In the DHCP snap-in, select a DHCP scope then right click on *Scope Options* then select *Configure Options*:



- Select the *Advanced* tab then under *Vendor class* select the Vendor Class name to assign to the DHCP scope. Click *OK*:



10 The Vendor Class and Options have now been assigned to a DHCP scope supporting the Access Points Native VLAN at one remote site:



### 2.8.3.4 Motorola WiNG 5.X

A Motorola WiNG 5.X Independent Access Point can be configured to provide DHCP services for a site. For DHCP services to be provided by an Independent Access Point, the Access Point must have a virtual IP interface defined with a static IP address for each VLAN the Access Point is providing DHCP services for. As each remote site will be assigned unique IP addressing, a separate DHCP policy will be required for each remote site.

Use the following procedure to create a DHCP Policy and Pool in WiNG 5.X which can be applied to a individual remote Access Point as a Device Override:

#### 1 Create a DHCP server policy and define option 191:

```
rfs6000-1(config)# dhcp-server-policy default
rfs6000-1(config-dhcp-policy-default)# option ControllerIPAddress 191 ascii
```

#### 2 Create a DHCP pool for the Access Points Native VLAN and define the required parameters and standard options:

```
rfs6000-1(config-dhcp-policy-default)# dhcp-pool VLAN21
rfs6000-1(config-dhcp-policy-default-pool-VLAN21)# network 192.168.21.0/24
rfs6000-1(config-dhcp-policy-default-pool-VLAN21)# address range 192.168.21.100 192.168.21.254
rfs6000-1(config-dhcp-policy-default-pool-VLAN21)# default-router 192.168.21.1
rfs6000-1(config-dhcp-policy-default-pool-VLAN21)# option ControllerIPAddress
pool1=192.168.20.22,192.168.20.23;level=2
rfs6000-1(config-dhcp-policy-default-pool-VLAN21)# exit
rfs6000-1(config-dhcp-policy-default)# exit
```

#### 3 Assign the DHCP Policy to an Access Point at the site as an Override:

```
rfs6000-1(config)# ap6532 5C-0E-8B-A4-48-80
rfs6000-1(config-device-5C-0E-8B-33-D3-4C)# use dhcp-server-policy default
rfs6000-1(config-device-5C-0E-8B-33-D3-4C)# end
```

#### 4 Commit and Write the Changes:

```
rfs6000-1# commit write
```

## 2.9 Pre-Staging Access Points

Use the following procedure to pre-stage an Independent Access Point using the Command Line Interface. Once adopted the Independent Access Points pre-staged configuration will be added to the Access Points Device configuration as Overrides:

### 1 Login to the Access Point and enter the default credentials *admin / motorola*. When prompted enter and confirm a new password:

```
ap6532-99B67C login: admin
```

```
Password: motorola
```

System is currently using the factory default login credentials.  
Please change the default password to protect from unauthorized access.

```
Enter new password: hellomoto
```

```
Confirm new password: hellomoto
```

Password for user 'admin' changed successfully.  
Please write this password change to memory(write memory) to be persistent

### 2 Access the device configuration and define a *hostname* for the Access Point. In this example the hostname *ap7131-1* is defined:

```
ap6532-99B67C> enable
```

```
ap6532-99B67C# self
```

```
ap6532-99B67C(config-device-00-23-68-99-B6-7C) # hostname ap6532-1
```

### 3 Access the *ge1* interface and assign a *Native* and *Tagged* VLANs. In this example the *Native* VLAN *21* and tagged VLANs *22-25* are defined:

```
ap6532-99B67C(config-device-00-23-68-99-B6-7C) # interface ge 1
```

```
ap6532-99B67C(config-device-00-23-68-99-B6-7C-if-ge1) # switchport mode trunk
```

```
ap6532-99B67C(config-device-00-23-68-99-B6-7C-if-ge1) # switchport trunk native vlan 21
```

```
ap6532-99B67C(config-device-00-23-68-99-B6-7C-if-ge1) # switchport trunk allowed vlan 21-25
```

```
ap6532-99B67C(config-device-00-23-68-99-B6-7C-if-ge1) # exit
```

### 4 Create a Virtual IP interface for the *Native* VLAN and assign a static *IP* address and *Subnet Mask*. In this example the static IP address *192.168.21.50/24* is defined:

```
ap6532-99B67C(config-device-00-23-68-99-B6-7C) # interface vlan 21
```

```
ap6532-99B67C(config-device-00-23-68-99-B6-7C-if-vlan21) # ip address 192.168.21.50/24
```

```
ap6532-99B67C(config-device-00-23-68-99-B6-7C-if-vlan21) # exit
```

### 5 Define a *Default Gateway*. In this example the default gateway for the *Native* VLAN *192.168.21.1* is defined:

```
ap6532-99B67C(config-device-00-23-68-99-B6-7C) # ip default-gateway 192.168.21.1
```

## 6 Define static *Controller Host* entries for the *Primary* and *Secondary* Wireless Controllers in the data center / NOC. In this example static *Level 2* links to *192.168.20.22* and *192.168.20.23* are defined:

```
ap6532-99B67C (config-device-00-23-68-99-B6-7C) # controller host 192.168.20.22 level 2
ap6532-99B67C (config-device-00-23-68-99-B6-7C) # controller host 192.168.20.23 level 2
```

## 7 Verify the configuration:

```
ap6532-99B67C (config-device-00-23-68-99-B6-7C) # show context

ap6532 00-23-68-99-B6-7C
  use profile default-ap6532
  use rf-domain default
  hostname ap6532-1
  ip default-gateway 192.168.21.1
  interface ge1
    switchport mode trunk
    switchport trunk native vlan 21
    no switchport trunk native tagged
    switchport trunk allowed vlan 21-25
  interface vlan21
    ip address 192.168.21.50/24
  logging on
  logging console warnings
  logging buffered warnings
  controller host 192.168.20.23 level 2
  controller host 192.168.20.22 level 2
```

## 8 Commit and Save the changes:

```
ap6532-99B67C (config-device-00-23-68-99-B6-7C) # commit write
```

## 9 On the Wireless Controllers in the data center / NOC, view the running configuration and verify that the remote Access Point has been discovered and its Device configuration added:

```
rfs6000-1# show running-config | begin 00-23-68-99-B6-7C
```

```
!
ap6532 00-23-68-99-B6-7C
  use profile store101-ap6532
  use rf-domain store101
  hostname ap6532-1
  ip default-gateway 192.168.21.1
  interface vlan21
    ip address 192.168.21.50/24
  controller host 192.168.20.23 level 2
  controller host 192.168.20.22 level 2
!
```

Device Overrides inherited from the newly discovered AP6532 Access Point from pre-staging. Note that the ge1 interface configuration in this example is not inherited as it matches the ge1 configuration already defined in the AP6532 Profile.

## 3. Verification

### 3.1 Verifying Adoption Status

Issue the **show adoption info** command to view basic adoption information about the Access Points adopted by the Wireless Controllers in the data center / NOC: From the available information you can quickly identify the **Total Number** of adopted Access Points as well as the **Type** and **Model** of each Access Point:

```
rfs6000-1# show adoption info
```

| HOST-NAME    | MAC               | TYPE   | MODEL            |
|--------------|-------------------|--------|------------------|
| store100-ap1 | 5C-0E-8B-A4-48-80 | ap6532 | AP-6532-66030-US |
| store100-ap2 | 5C-0E-8B-A4-4B-48 | ap6532 | AP-6532-66030-US |
| store100-ap3 | 5C-0E-8B-A4-4C-3C | ap6532 | AP-6532-66030-US |
| store101-ap1 | 00-23-68-97-04-DC | ap6532 | AP-6532-66030-US |
| store101-ap2 | 00-23-68-99-B6-7C | ap6532 | AP-6532-66030-US |
| store101-ap3 | 00-23-68-99-B9-30 | ap6532 | AP-6532-66030-US |

Total number of APs displayed: 6



Tip – You can quickly filter the output of a command using **grep** to look for specific information. For example issuing the **show adoption info | grep store100** command will display all the Access Points adopted from store 100.

Issue the **show adoption status** command to view detailed adoption information about the Access Points adopted by the Wireless Controllers in the data center / NOC. From the available information you can quickly identify which of the Wireless Controllers each Access Point is **Adopted By** as well as identify each Access Points **Configuration State**, **Uptime** and **Firmware Version**:

```
rfs6000-1# show adoption status
```

| HOST-NAME    | VERSION      | CFG STAT   | ADOPTED-BY | LAST-ADOPTION       | UPTIME          |
|--------------|--------------|------------|------------|---------------------|-----------------|
| store100-ap1 | 5.2.0.0-069R | configured | rfs6000-1  | 2011-10-04 11:12:30 | 0 days 00:27:03 |
| store100-ap2 | 5.2.0.0-069R | configured | rfs6000-2  | 2011-10-04 11:12:15 | 0 days 00:27:03 |
| store100-ap3 | 5.2.0.0-069R | configured | rfs6000-2  | 2011-10-04 11:12:15 | 0 days 00:27:03 |
| store101-ap1 | 5.2.0.0-069R | configured | rfs6000-2  | 2011-10-04 11:34:55 | 0 days 00:05:14 |
| store101-ap2 | 5.2.0.0-069R | configured | rfs6000-1  | 2011-10-04 11:35:07 | 0 days 00:05:11 |
| store101-ap3 | 5.2.0.0-069R | configured | rfs6000-1  | 2011-10-04 11:36:13 | 0 days 00:05:13 |

Total number of APs displayed: 6

## 3.2 Verifying RF Domains

Issue the **show noc device** command to view the **Online** status of the known Wireless Controllers and Access Points in the Wireless System as well as **RF Domain** assignments. Each Wireless Controller in the data center / NOC should be assigned to a common RF Domain while Access Points should be assigned to one common RF Domain per site:

```
rfs6000-1# show noc device
```

| MAC               | HOST-NAME    | TYPE    | CLUSTER | RF-DOMAIN | ADOPTED-BY        | ONLINE |
|-------------------|--------------|---------|---------|-----------|-------------------|--------|
| 00-23-68-64-43-5A | rfs6000-1    | rfs6000 | noc     | noc       |                   | online |
| 5C-0E-8B-17-E8-F6 | rfs6000-2    | rfs6000 | noc     | noc       |                   | online |
| 5C-0E-8B-A4-48-80 | store100-ap1 | ap6532  |         | store100  | 00-23-68-64-43-5A | online |
| 5C-0E-8B-A4-4B-48 | store100-ap2 | ap6532  |         | store100  | 5C-0E-8B-17-E8-F6 | online |
| 5C-0E-8B-A4-4C-3C | store100-ap3 | ap6532  |         | store100  | 5C-0E-8B-17-E8-F6 | online |
| 00-23-68-97-04-DC | store101-ap1 | ap6532  |         | store101  | 5C-0E-8B-17-E8-F6 | online |
| 00-23-68-99-B6-7C | store101-ap2 | ap6532  |         | store101  | 00-23-68-64-43-5A | online |
| 00-23-68-99-B9-30 | store101-ap3 | ap6532  |         | store101  | 00-23-68-64-43-5A | online |

Total number of clients displayed: 8

Issue the **show noc domain managers** command to view the elected RF Domain **Manager** for each of the defined RF Domains. One Access Point from each remote site will be elected and displayed. If the elected Access Point fails or is taken off-line, another Access Point at the site will be elected:

```
rfs6000-1# show noc domain managers
```

| RF-DOMAIN       | MANAGER                  | HOST-NAME           | APS      | CLIENTS  |
|-----------------|--------------------------|---------------------|----------|----------|
| noc             | 00-23-68-64-43-5A        | rfs6000-1           | 0        | 0        |
| noc             | 5C-0E-8B-17-E8-F6        | rfs6000-2           | 0        | 0        |
| <b>store100</b> | <b>5C-0E-8B-A4-48-80</b> | <b>store100-ap1</b> | <b>3</b> | <b>0</b> |
| <b>store101</b> | <b>00-23-68-97-04-DC</b> | <b>store101-ap1</b> | <b>3</b> | <b>0</b> |

Total number of RF-domain displayed: 4



Note – You can pre-select a specific Access Point as RF Domain Manager for a site by issuing the **rf-domain-manager priority** command as a device Override and assigning a priority value of **255**.



### 3.3 Verifying MINT

Issue the **show mint links** command on each of the Wireless Controllers in the data center / NOC to view the established VLAN and IP based MINT links. One Level 2 IP based MINT link will be present on each Wireless Controller for the cluster while one Level 2 IP based MINT link will be present to each elected RF Domain manager (one per site). In the example below one Level 2 IP based MINT link has been established to **rfs6000-1** from the elected RF Domain manager at **Store 100** while one Level 2 IP based MINT link has been established to **rfs6000-2** from the elected RF Domain manager at **Store 101**.

```
rfs6000-1# show mint links on rfs6000-1
```

```
2 mint links on 68.64.43.5A:
```

```
link ip-192.168.20.23:24576 at level 2, 1 adjacencies, forced
```

```
link ip-192.168.21.102:24576 at level 2, 1 adjacencies, (used)
```

```
rfs6000-2# show mint links on rfs6000-2
```

```
2 mint links on 68.64.43.5A:
```

```
link ip-192.168.20.22:24576 at level 2, 1 adjacencies, forced
```

```
link ip-192.168.31.100:24576 at level 2, 1 adjacencies, (used)
```

Issue the **show mint links** command on each of the Access Points at a specific site. Each Access Point will have an established Level 1 VLAN based MINT link to its neighboring Access Points over its Native VLAN (control VLAN) while only the elected RF Domain manager at the site will display a **used** Level 2 IP based MINT link to the Wireless Controllers in the data center / NOC. Non RF Domain managers will display the Level 2 IP based MINT link but will list it as **unused**.

```
rfs6000-1# show mint links on store100-ap1
```

```
2 mint links on 68.64.43.5A:
```

```
link vlan-21 at level 1, 2 adjacencies, DIS 0B.A4.4B.48
```

```
link ip-192.168.20.23:24576 at level 2, 1 adjacencies, (used)
```

```
rfs6000-1# show mint links on store100-ap2
```

```
2 mint links on 68.64.43.5A:
```

```
link vlan-21 at level 1, 2 adjacencies, DIS 0B.A4.4B.48
```

```
link ip-192.168.20.22:24576 at level 2, 0 adjacencies, (unused)
```

```
rfs6000-1# show mint links on store100-ap3
```

```
2 mint links on 68.64.43.5A:
```

```
link vlan-21 at level 1, 2 adjacencies, DIS 0B.A4.4B.48
```

```
link ip-192.168.20.23:24576 at level 2, 0 adjacencies, (unused)
```

Issue the **show mint id on <device-name>** command to identify the MINT ID of the RF Domain Manager and one of the other Access Points at a remote site:

```
rfs6000-1# show mint id of store100-ap1
```

Mint ID: **0B.A4.48.80**

```
rfs6000-1# show mint id of store100-ap2
```

Mint ID: **0B.A4.4B.48**

Issue the **mint traceroute <mint-id>** command against both the RF Domain Manager and non RF Domain Manager MINT IDs. You will notice that to reach the non RF Domain Manager Access Point at the remote site (forward and reverse), the MINT packets have to go through the elected RF Domain manager at the site.

In the example below for the Wireless Controller can reach the elected RF Domain Manager with the MINT id **0B.A4.4B.80** directly. However for the Wireless Controllers to reach the non RF Domain Manager with the MINT id **0B.A4.4B.48**, it has to go through the elected RF Domain Manager with the MINT id **0B.A4.4B.80**:

```
rfs6000-1# mint traceroute 0B.A4.4B.80
```

| DIR | MINT-ADDRESS | MAC-ADDRESS       | L2-gw | LEVEL | PRODUCT-TYPE | RF-DOMAIN | HOSTNAME     |
|-----|--------------|-------------------|-------|-------|--------------|-----------|--------------|
| F   | 68.64.43.5A  | 00-23-68-64-43-5A | Y     | L1/L2 | RFS6000      | noc       | rfs6000-1    |
| D   | 0B.A4.48.80  | 5C-0E-8B-A4-48-80 | Y     | L1/L2 | AP6532       | store100  | store100-ap1 |
| R   | 68.64.43.5A  | 00-23-68-64-43-5A | Y     | L1/L2 | RFS6000      | noc       | rfs6000-1    |

```
rfs6000-1# mint traceroute 0B.A4.4B.48
```

| DIR | MINT-ADDRESS | MAC-ADDRESS       | L2-gw | LEVEL | PRODUCT-TYPE | RF-DOMAIN | HOSTNAME     |
|-----|--------------|-------------------|-------|-------|--------------|-----------|--------------|
| F   | 68.64.43.5A  | 00-23-68-64-43-5A | Y     | L1/L2 | RFS6000      | noc       | rfs6000-1    |
| F   | 0B.A4.48.80  | 5C-0E-8B-A4-48-80 | Y     | L1/L2 | AP6532       | store100  | store100-ap1 |
| D   | 0B.A4.4B.48  | 5C-0E-8B-A4-4B-48 | N     | L1/L2 | AP6532       | store100  | store100-ap2 |
| R   | 0B.A4.48.80  | 5C-0E-8B-A4-48-80 | Y     | L1/L2 | AP6532       | store100  | store100-ap1 |
| R   | 68.64.43.5A  | 00-23-68-64-43-5A | Y     | L1/L2 | RFS6000      | noc       | rfs6000-1    |

## 4. Appendix

### 4.1 Scaling

The following section provides important scaling information which can be used to correctly design and implement a NOC deployment.

#### 4.1.1 Sites and Access Points

The following tables provide the maximum number of remote sites and Access Points which can be supported per Wireless Controller model for both the WiNG 5.2 and WiNG 5.3 releases. Each Wireless Controller is designed to support a specific number of Independent Access Points and is licensed accordingly. The appropriate number of licenses will need to be purchased and installed to support your specific deployment. Access Point licenses are shared within the Cluster.

When designing for redundancy it is also important to ensure that you don't exceed the maximum number of sites or the adoption capacity for each Wireless Controller. For example if you have 100 remote sites with 256 total Access Points split between two RFS6000 Wireless Controllers and a failure occurs, you will exceed the number of supported sites on a single RFS6000 Wireless Controller. An RFS7000 Wireless Controller for this deployment would be a better choice.

| Wireless Controller Model | Maximum Number of Sites | Maximum APs |
|---------------------------|-------------------------|-------------|
| RFS6000                   | 64                      | 256         |
| RFS7000                   | 256                     | 1,024       |
| NX9000                    | 4,096                   | 10,240      |

**Table 4.1.1.1 – WiNG 5.2 Sites / APs**

| Wireless Controller Model | Maximum Number of Sites | Maximum APs |
|---------------------------|-------------------------|-------------|
| RFS6000                   | 256                     | 256         |
| RFS7000                   | 1,024                   | 1,024       |
| NX9000                    | 4,096                   | 10,240      |

**Table 4.1.1.2 – WiNG 5.3 Sites / APs**

## 4.1.2 Wireless Users

The following tables provide the maximum number of wireless users which can be supported per Wireless Controller model and Access Point Radio in a WiNG 5.X deployment. Please note that while each Access Point radio can support up to 256 users, it is not recommended to exceed 50 users:

| Wireless Controller Model | Maximum Wireless Users / Controller |
|---------------------------|-------------------------------------|
| RFS6000                   | 4,096                               |
| RFS7000                   | 16,484                              |
| NX9000                    | 32,968                              |

**Table 4.1.2.1 – Wireless Users / Controller**

| Access Point Model | Maximum Wireless Users / Radio |
|--------------------|--------------------------------|
| AP6511             | 256                            |
| AP6521             | 256                            |
| AP6532             | 256                            |
| AP7131             | 256                            |
| AP7161             | 256                            |

**Table 4.1.2.2 – Wireless Users / Access Point Radio**

## 4.1.3 Wireless LANs

The following table provides the maximum number of Wireless LANs which can be defined per Wireless Controller model in a WiNG 5.X deployment. In a NOC model it will be typical to deploy a common set of Wireless LANs across all sites requiring only a small number of Wireless LANs to be defined. If a Wireless LAN on a specific site requires a unique SSID or VLAN assignment, this can be performed by assigning an Override to the RF Domain rather than defining a separate Wireless LAN:

| Wireless Controller Model | Maximum WLANs |
|---------------------------|---------------|
| RFS6000                   | 32            |
| RFS7000                   | 256           |
| NX9000                    | 1,024         |

**Table 4.1.3 – Wireless LANs**

## 4.1.4 Profiles

The following table provides the maximum aggregate number of Device Profiles which can be defined per Wireless Controller model in a WiNG 5.X deployment. Each WiNG 5.X Wireless Controller can only support a total number of 256 Device Profiles which includes Device Profiles for Controllers and Access Points:

| Wireless Controller Model | Maximum Aggregate Profiles |
|---------------------------|----------------------------|
| RFS6000                   | 256                        |
| RFS7000                   | 256                        |
| NX9000                    | 256                        |

**Table 4.1.4 – Profiles**

## 4.1.5 Policies

The following table provides the maximum number of Policies of each type which can be defined in a WiNG 5.X deployment:

| Policies   | Maximum Policies |
|--|------------------|
| <ul style="list-style-type: none"> <li>▪ Smart RF Policies</li> <li>▪ Radio QoS Policies</li> <li>▪ WIPS Policies</li> <li>▪ IP Firewall Rules</li> <li>▪ MAC Firewall Rules</li> <li>▪ User Roles</li> <li>▪ Automatic Provisioning Policies</li> <li>▪ Device Categorization Policies</li> </ul> | 256 (Each)       |
| <ul style="list-style-type: none"> <li>▪ WLAN QoS Policies</li> <li>▪ AAA Policies</li> <li>▪ Associated ACL Policies</li> <li>▪ Captive Portal Policies</li> <li>▪ DNS Whitelists</li> </ul>  | 32 (Each)        |
| <ul style="list-style-type: none"> <li>▪ Management Policies</li> <li>▪ DHCP Server Policies</li> <li>▪ RADIUS Server Policies</li> <li>▪ RADIUS User Pools</li> </ul>   | 64 (Each)        |

**Table 4.1.5 – Policies**

## 4.1.6 RF Domain Manager

The following table provides the maximum number of Access Points that can be supported per model of Access Point providing RF Domain Manager services. Each RF Domain Manager can support Access Points of the same model as well as Access Points of different models (mixed deployments):

| RF Domain Manager | Maximum APs / Site |
|-------------------|--------------------|
| AP6511            | 24                 |
| AP6521            | 24                 |
| AP6532            | 24                 |
| AP7131            | 36                 |
| AP7161            | 36                 |

**Table 4.1.6 – APs / RF Domain Manager**

## 4.2 Bandwidth Requirements

In a NOC deployment remote sites can be connected to the data center / NOC using a variety of WAN technologies and services. Most deployments will utilize a private WAN or MPLS service which provide dedicated bandwidth from each remote site. However other deployments may utilize xDSL, DOCSIS or 3G/4G services over the public Internet either for primary WAN connectivity or backup WAN connectivity. Some deployments may utilize a mixture of all technologies depending on which services are available at each site.

The following table provides the recommended minimum bandwidth, latency and MTU recommendations required to support remote Access Points with the NOC model. These values are intended as a basic guidelines only as the deployed applications and number of devices at a remote site will ultimately determine the bandwidth and latency requirements for the site:

| WAN Characteristic | Minimum    |
|--------------------|------------|
| Minimum Bandwidth  | 256 Kbps   |
| Maximum Latency    | < 2,000 ms |
| Minimum MTU        | 900 Bytes  |

**Table 4.2.1 – WAN Recommendations**

The NOC model outlined in this guide is optimized for WAN deployments and Access Points at remote sites require a very small amount of bandwidth to operate and communicate with the Wireless Controllers in the data center / NOC. During normal operation statistics and site information is forwarded through the elected RF Domain Manager at the site and each Access Point requires 2 – 4kbps of bandwidth to function. A site with 24 remote Access Points will require no more than 96kbps of bandwidth during normal operation. If Sensor radios are deployed for AirDefense Advanced WIPS, an additional 3 – 5Kbps of bandwidth will be required per Sensor radio:

| Access Point Type | Typical Bandwidth             |
|-------------------|-------------------------------|
| Access Points     | 2 - 4 Kbps (Per AP)           |
| Sensor Radio      | 3 - 5 Kbps (Per Sensor Radio) |

**Table 4.2.2 – Typical Bandwidth Requirement**

By default frequency of RF Domain Manager → Controller updates are automatically determined based on the number of remote sites. Typically an RF Domain Manager at a remote site will update the Controllers in the data center / NOC once per minute. The update interval can be configured by changing the ***noc update-interval*** value **<5-3600>** in seconds on the Wireless Controllers. A shorter update-interval will result in more WAN bandwidth being required to support each remote site.

When Access Points at remote sites boot and receive their initial configuration they will require a small amount of additional bandwidth while the configuration parameters are pushed from the Controllers to the remote Access Points. Additional bandwidth will also be required when configuration changes are applied to a site. However the additional bandwidth in both these cases is small and inconsequential.

When firmware image updates are applied to a remote site, the firmware is pushed to the elected RF Domain Manager at the site which co-ordinates the firmware upgrades to Access Points at the site. An RF Domain Manager will upgrade other Access Point models first and will update its own Access Point type as well as itself last.

The following table provides the firmware image sizes for each Access Point in the 5.2.0.0-069R release:

| Access Point Model | Firmware Image Size |
|--------------------|---------------------|
| AP6511             | 17,193,190 bytes    |
| AP6521             | 17,932,851 bytes    |
| AP6532             | 15,595,885 bytes    |
| AP71xx             | 17,748,208 bytes    |

**Table 4.2.3 – WiNG 5.2 Firmware Image Size**



## 4.3 WiNG 5.X Protocols & Ports

The following table provides the Protocols and Ports supported by Independent Access Points. If firewalls are deployed between the remote Access Points and Wireless Controllers in the data center / NOC, UDP port 24576 must be permitted or adoption will fail. Additional protocols and ports may need to be permitted for AAA and Management depending on each specific deployment requirements:

| Protocol | Port   | Description   |
|----------|--------|---|
| TCP      | 20-21  | FTP File Transfers.                                     |
| TCP      | 22     | SSHv2 Device Management.                                |
| TCP      | 23     | Telnet Device Management.                               |
| TCP      | 49     | TACACS+ Authentication.                                 |
| UDP      | 53     | DNS Name Resolution.                                    |
| UDP      | 69     | TFTP File Transfers.                                    |
| TCP      | 80     | HTTP Device Management.                                 |
| UDP      | 123    | NTP Time Synchronization.                               |
| UDP      | 161    | SNMP Device Management.                                 |
| UDP      | 162    | SNMP Traps.   |
| TCP      | 389    | LDAP / Active Directory Authentication.                 |
| TCP      | 443    | HTTPS Device Management / Sensor → ADSP Communications. |
| TCP      | 444    | HTTPS Captive Portal Authentication.                    |
| TCP      | 880    | HTTP Captive Portal Authentication.                     |
| UDP      | 1,812  | RADIUS Authentication.                                  |
| UDP      | 1,813  | RADIUS Accounting.                                      |
| TCP      | 8,443  | Sensor → Controller Communications (Advanced WIPS).     |
| UDP      | 24,576 | Access Point Adoption ( <b>Mandatory</b> ).             |

**Table 4.3 – WiNG 5.X Protocols & Ports**

## 4.4 Running Configuration

```
!  
! Configuration of RFS6000 version 5.2.0.0-069R  
!  
!  
version 2.1  
!  
!  
!  
mac access-list PERMIT-ARP-AND-IPv4  
    permit any any type ip rule-precedence 10 rule-description "permit all IPv4 traffic"  
    permit any any type arp rule-precedence 20 rule-description "permit all ARP traffic"  
!  
firewall-policy default  
    no ip dos tcp-sequence-past-window  
!  
igmp-snoop-policy default  
    no igmp-snooping  
    no querier  
    unknown-multicast-fwd  
!  
!  
mint-policy global-default  
!  
wlan-qos-policy default  
    qos trust dscp  
    qos trust wmm  
!  
radio-qos-policy default  
!  
aaa-policy external-aaa  
    authentication server 1 host 192.168.10.10 secret 0 hellomoto  
    authentication server 2 host 192.168.10.11 secret 0 hellomoto  
!  
wlan STORES-DOT1X  
    ssid STORES-DOT1X  
    vlan 22  
    bridging-mode local  
    encryption-type ccmp  
    authentication-type eap  
    use aaa-policy external-aaa
```

```
!  
wlan STORES-PSK  
  ssid STORES-PSK  
  vlan 23  
  bridging-mode local  
  encryption-type ccmp  
  authentication-type none  
  wpa-wpa2 psk 0 hellomoto  
!  
auto-provisioning-policy noc  
  adopt ap6532 precedence 1 profile stores-ap6532 rf-domain store100 ip 192.168.21.0/24  
  adopt ap6532 precedence 2 profile stores-ap6532 rf-domain store101 ip 192.168.31.0/24  
!  
!  
management-policy default  
  no http server  
  https server  
  ssh  
  user admin password 0 motorola role superuser access all  
  user operator password 0 motorola role monitor access all  
  no snmp-server manager v2  
  snmp-server community public ro  
  snmp-server community private rw  
  snmp-server user snmpoperator v3 encrypted des auth md5 0 operator  
  snmp-server user snmptrap v3 encrypted des auth md5 0 motorola  
  snmp-server user snmpmanager v3 encrypted des auth md5 0 motorola  
!  
management-policy noc  
  no http server  
  https server  
  ssh  
  user admin password 0 hellomoto role superuser access all  
!  
management-policy stores  
  no http server  
  ssh  
  user admin password 0 hellomoto role superuser access all  
!  
profile rfs6000 noc-rfs6000  
  ip name-server 192.168.10.5  
  ip domain-name tmelabs.local  
  no autoinstall configuration
```

```
no autoinstall firmware
crypto isakmp policy default
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
interface me1
interface up1
    description Uplink
    switchport mode trunk
    switchport trunk native vlan 20
    switchport trunk native tagged
    switchport trunk allowed vlan 20
    ip dhcp trust
    qos trust dscp
    qos trust 802.1p
interface ge1
    ip dhcp trust
    qos trust dscp
    qos trust 802.1p
interface ge2
    ip dhcp trust
    qos trust dscp
    qos trust 802.1p
interface ge3
    ip dhcp trust
    qos trust dscp
    qos trust 802.1p
interface ge4
    ip dhcp trust
    qos trust dscp
    qos trust 802.1p
interface ge5
    ip dhcp trust
    qos trust dscp
    qos trust 802.1p
interface ge6
    ip dhcp trust
    qos trust dscp
    qos trust 802.1p
interface ge7
    ip dhcp trust
    qos trust dscp
    qos trust 802.1p
interface ge8
```

```
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface wwan1
use management-policy noc
use firewall-policy default
use auto-provisioning-policy noc
ntp server 192.168.10.5
service pm sys-restart
!
profile ap6532 stores-ap6532
ip name-server 192.168.10.5
ip domain-name tmelabs.local
no autoinstall configuration
no autoinstall firmware
interface radiol
wlan STORES-PSK bss 1 primary
wlan STORES-DOT1X bss 2 primary
interface radio2
wlan STORES-DOT1X bss 1 primary
interface gel
description Uplink
switchport mode trunk
switchport trunk native vlan 21
no switchport trunk native tagged
switchport trunk allowed vlan 21-23
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface vlan21
description AP\ VLAN
ip address dhcp
ip dhcp client request options all
use management-policy stores
use firewall-policy default
ntp server 192.168.10.5
service pm sys-restart
!
rf-domain default
no country-code
!
rf-domain noc
```

```
location SanJoseCA
contact admin@tmelabs.local
timezone PST8PDT
country-code us
!
rf-domain store100
location SanJoeCA
contact admin@tmelabs.local
timezone PST8PDT
country-code us
control-vlan 21
!
rf-domain store101
location PleasontonCA
contact admin@tmelabs.local
timezone PST8PDT
country-code us
control-vlan 21
!
rfs6000 00-23-68-64-43-5A
use profile noc-rfs6000
use rf-domain noc
hostname rfs6000-1
license AP <license-string>
license AAP <license-string>
license ADVANCED-WIPS <license-string>
license ADSEC <license-string>
ip default-gateway 192.168.20.1
interface mel
    ip address 192.168.0.1/24
interface vlan20
    description Management
    ip address 192.168.20.22/24
cluster name noc
cluster member ip 192.168.20.23 level 2
cluster master-priority 255
logging on
logging console warnings
logging buffered warnings
!
rfs6000 5C-0E-8B-17-E8-F6
use profile noc-rfs6000
```

```
use rf-domain noc
hostname rfs6000-2
ip default-gateway 192.168.20.1
interface vlan20
    description Management
    ip address 192.168.20.23/24
cluster name noc
cluster member ip 192.168.20.22 level 2
cluster master-priority 100
!
ap6532 5C-0E-8B-A4-48-80
    use profile stores-ap6532
    use rf-domain store100
    hostname store100-ap1
!
ap6532 5C-0E-8B-A4-4B-48
    use profile stores-ap6532
    use rf-domain store100
    hostname store100-ap2
!
ap6532 5C-0E-8B-A4-4C-3C
    use profile stores-ap6532
    use rf-domain store100
    hostname store100-ap3
!
ap6532 00-23-68-97-04-DC
    use profile stores-ap6532
    use rf-domain store101
    hostname store101-ap1
!
ap6532 00-23-68-99-B6-7C
    use profile stores-ap6532
    use rf-domain store101
    hostname store101-ap2
!
ap6532 00-23-68-99-B9-30
    use profile stores-ap6532
    use rf-domain store101
    hostname store101-ap3
!
!
end
```





