# Table of Contents

1. Introduction .......................................................................................................................................... 5
   1.1 Architecture ........................................................................................................................................ 6
   1.2 Forwarding .......................................................................................................................................... 9
   1.3 Radius Redundancy ........................................................................................................................... 10
2. Configuration ...................................................................................................................................... 11
   2.1 RF Domains ....................................................................................................................................... 13
   2.2 Management Policies ........................................................................................................................ 16
   2.3 Smart-RF............................................................................................................................................ 21
   2.4 Wireless Intrusion Prevention (WIPS) ............................................................................................. 24
   2.5 Wireless LANs.................................................................................................................................... 28
   2.6 Profiles .............................................................................................................................................. 40
   2.7 Radius Server .................................................................................................................................... 57
   2.8 Role Based Access Control ................................................................................................................ 64
   2.9 Clustering .......................................................................................................................................... 70
   Device Overrides ..................................................................................................................................... 70
   2.9.1 Wireless Controller (Cluster Master) ........................................................................................... 70
   2.9.2 Cluster Member Switch ................................................................................................................ 76
   2.10 Auto Provisioning Policies ............................................................................................................... 82
   2.11 Forming the Cluster ........................................................................................................................ 87
3. Verification.............................................................................................................................................. 88
   3.1 Verifying Adoption Status ................................................................................................................. 89
   3.2 Verifying RF Domains ...................................................................................................................... 89
   3.3 Verifying MINT ................................................................................................................................. 90
   3.4 Verifying Smart-RF ........................................................................................................................... 91
4. Appendix .............................................................................................................................................. 92
   4.1 Scaling .............................................................................................................................................. 92
   4.1.1 Access Points ............................................................................................................................... 93
   4.1.2 Wireless Users ............................................................................................................................. 95
   4.1.3 Wireless LANs ............................................................................................................................... 96
4.1.4 DHCP Server support ...............................................................................................................................96
4.1.5 Firewall ACL rules .................................................................................................................................97
4.1.6 Firewall flows .......................................................................................................................................97
4.1.7 Profiles .................................................................................................................................................98
4.1.8 MAC address table size .......................................................................................................................99
4.2 VLAN planning .......................................................................................................................................99
4.3 WiNG 5.X Protocols & Ports ..................................................................................................................100
1. Introduction

Zebra Technologies provides a highly scalable centrally managed Wireless LAN solution for customers deploying 802.11n Wireless LAN services in a Campus environment, like Enterprise, Education and Healthcare. In a typical campus deployment, the Wireless controllers and a number of access points are deployed in a private network spread across multiple floors or buildings. The Wireless Controllers are installed at the data center and the access points are deployed across the campus. The configuration and management is performed by the Zebra Wireless Controllers.

The Wireless user traffic can either be tunneled to the wireless controller or bridged locally by the access point towards its destination. The local forwarding mode eliminates the latency of routing the traffic through the wireless controller and unnecessary overload on the wireless controller. The tunnel forwarding mode could be used in case the user traffic needs to be mapped to VLANs which are not extended across the campus at the AP location, or to provide seamless mobility even as the users roam across access points deployed across multiple VLANs.

You can deploy the dependent APs for most campus deployments, with two wireless controllers working in high availability mode. Zebra offers various Wireless controllers and Access Point models to suit the needs of various enterprise requirements. The number of access points that can be supported depends on the controller model and the forwarding mode, as we will discuss later (in section 4.1). Each Access Point can provide full QoS (Quality of Service), security and mobility by itself, without tunneling the traffic through the wireless controller.
1.1 Architecture

The Zebra Technologies campus deployment model utilizes a cluster of Wireless Controllers in the data center. The access points are distributed across the campus over various floors and buildings. The access points can be on the same VLAN as the controller, or they can be across multiple subnets, across a routed network from the controller. In either case, the access point shares the same RF-Domain as the wireless controller.

The access points are adopted to the wireless controller which manages all the access points wrt pushing the AP configuration, firmware upgrades, Smart-RF operation and statistics collection. In case some WLANs are tunneling user traffic over extended VLANs, the data traffic can be adaptively forwarded to the wireless controller or any other access point directly, whichever is the shorter path.

The access points can be adopted to the wireless controller over Layer 2 (same VLAN) or Layer 3 (routed subnet):

- **L2 adoption**: The Wireless Controllers and access points share the same VLAN. The APs automatically discover the controller, gets adopted and the controller pushes the AP configuration based on the auto provisioning policies (described in section 2.11)

- **L3 adoption**: When the Controller VLAN cannot be extended to the AP, the APs can use Layer 3 adoption to be managed by the controller in a different routed subnet. Since the wireless controller is not present on the same subnet, the APs cannot discover the controllers automatically. The controller IP address should be provided to the APs, either with manual configuration, or using DHCP option 191. When the APs get IP address using DHCP service, they will also learn the controller IP address through the DHCP option 191.
The following describes how the Access Points and Wireless Controllers communicate in the Campus deployment model:

1) The Wireless Access Points automatically discover the Wireless Controllers in the same VLAN using MINT MLCP Discovery or DHCP option 191. The Access Points can be load-balanced across the controllers in the cluster and adopt to the least loaded Wireless Controller. Alternately, they can be steered to a specific Wireless Controller using the Preferred Controller Group name.

2) Once a 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.

3) The Access Points discover their neighboring Access Points and share control information with each other that helps in fast roaming, load balancing wireless clients across channels, bands and access points.

The Wireless Controllers manage all functions for the access points from firmware upgrade, configuration push, smart-rf management, etc.

For plug-n-play Access Point deployments it is recommended that the Native VLAN ID should be configured as untagged on the Ethernet switch port to which the Access Points are connected. As new Access Points are connected to the Ethernet ports, they will automatically discover the controllers on their default VLAN 1.

By configuring the Native VLAN as untagged permits Controller discovery and will allow a new Access Point to adopt and receive its configuration. The access point will discover the controller on it’s native VLAN using MINT MLCP discovery. If the controller is not present on the same VLAN, the Access Point will obtain DHCP addressing over VLAN 1, discover the Wireless Controllers using DHCP option 191, adopt and receive their configuration which includes the new Native VLAN ID. Once received the Access Point would adopt to the new controller and continue to operate.
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.

**Manual Configuration:**
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 to receive their configuration. In such a scenario, it will be required to manually configure the ge1 port of the access point to have the native vlan as tagged. And match the 802.1q configuration on the Ethernet switch port.

As described above that the Access point can automatically discover the controller on the same VLAN using MINT MLCP discovery and using DHCP option 191 when the controller is on a different subnet. If the Wireless controller is in a different subnet, and no DHCP server is present, or does not support option configuration, then the Wireless Controller IP addresses or hostnames can be defined on each Access Point manually. It requires certain parameters to be pre-configured on the 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 Access Point is able to communicate across the subnet and discover the Wireless Controllers.
1.2 Forwarding

The access points can either bridge the traffic locally like an independent access point or will tunnel the traffic to the Wireless Controller in the data center or another access point, depending on where the traffic is destined to.

**Tunneled VLAN:**

If the wireless LAN users need to be mapped to a different VLAN than the VLAN currently extended on the wired network, the VLAN can be tunneled to the Wireless controller in the data center. The VLANs may also be tunneled to provide seamless mobility to the wireless users as they move across the campus, or to enforce access restrictions on the VLAN that the wireless devices are mapped to.

In such a scenario, it is not needed to extend the VLAN to each AP location across the wired network. The wireless users can be mapped to the tunneled VLAN from any location, irrespective of the VLAN currently mapped on the Ethernet switch port where the AP is connected to. All the user traffic is then tunneled through the best path to its destination. The best path could be through the wireless controllers or a neighboring access point. The neighbor here is referred to as the MINT neighbor.

802.1q tagging is not necessary since the user VLANs need not be trunked on the AP. Even if the users are mapped to multiple tunneled vlans, even then 802.1q tagging is not needed on the Access points.

**Locally bridged VLAN:**

Locally bridged VLAN is similar to the forwarding mode as used in an independent access point and the wireless controller is completely removed from the data path. The user traffic is mapped to the VLAN connected to the Ethernet port of the access points, and can be bridged or router directly to its destination.

If wireless users are mapped to multiple VLANs, 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.
1.3 Radius Redundancy

For Campus deployments, multiple redundant RADIUS AAA servers are deployed within the data center. However, for small deployments, RADIUS AAA service may also be provided using a WiNG 5.x device, which could be a controller or an access point. The WiNG 5.x device could also be used for redundancy as a secondary radius server.

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, or be forwarded through the Wireless Controllers managing the APs.

If the RADIUS server is unavailable for any reason, 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 which is backed up by a second RADIUS server either located in the same or alternate location.
2. Configuration

This section provides the necessary configuration steps required to provision a cluster of Wireless Controllers to support AP650 Access Point deployments within a campus environment. In the following configuration example two RFS7000 Wireless Controllers will be configured in the data center as an Active / Active cluster.

One user defined RF Domain will be defined for the site.

2 x RSF7000 will be configured in Active-active clustering mode.

Common configuration parameters and policies will be assigned to the RFS7000 Wireless Controllers and the AP650 Access Points using user defined Profiles.

A user defined Management Policy will be assigned to the Wireless Controllers and managed Access Points.

One 802.11i Wireless LAN and one guest access Wireless LAN will be defined and assigned to AP650 Access Point radios using the AP650 user defined Profile. A Captive portal policy is defined for the Guest access.

Role Based access control is configured to provide access to users based on their role.

Static IP addressing and cluster configuration will be assigned to each of the RFS7000 Wireless Controllers as Device overrides.

A Smart-RF policy is defined to ensure the wireless infrastructure adopts to dynamic changes to the RF environment.

An Auto-Provisioning Policy will be defined and assigned to the RFS7000 user defined profile.

Captive Portal policy is created for Guest access.

A Radius Server Policy is created for the Guest wireless users.

A WIPS policy is created to protect the wireless infrastructure from any intrusion attempts.

Configuration examples will be provided for both CLI and the Web User Interface.
Figure 2.1 Network Architecture

For this configuration example two RFS7000 series Wireless Controllers and AP650 Access Points are used. It’s important to note that these configuration steps are applicable to other Zebra Wireless Controllers and Access Points. Zebra offers a wide range of Access Points to suit diverse customer requirements. Please choose the access point and wireless controllers that is most appropriate for your requirements.

The 2 RFS7000s are deployed at the data center and the APs are distributed across the campus on multiple VLANs (VLAN 30 and 40). The VLAN 30 is extended from the wireless controllers in the data centre to the access layer. The VLAN 40 is assigned to the wired ports on Floor-2 and the access points are deployed on VLAN 40. The access points on VLAN 40 have Layer 3 (IP) connectivity to the wireless Controllers. The corporate users are mapped on the VLAN 100 and VLAN 110, based on their identity. The guest users are mapped on the VLAN 200. The radius servers are placed in the data centers and are used for the 802.1x authentication of the corporate users. The guest users are created on the wireless controllers and the onboard radius server on the wireless controllers is used for the guest user authentication. The DHCP server is assigning IP addresses to the wireless users on VLAN 100, VLAN 110 and VLAN 200.

It should be noted that the user VLAN 100, VLAN 110 and VLAN 200 is not extended across the wired infrastructure and to each AP. It is only terminated in the data center on the wireless controllers.

The default gateway for the wireless users is 172.16.100.1 for VLAN 100, 172.16.110.1 for VLAN 110 and 172.16.200.1 for VLAN 200, which is an external router and the controller is only bridging the user traffic for both wireless LANs.
Since the APs on floor-1 are deployed in the same VLAN as the controller (VLAN 30), the APs automatically discover the controller, gets adopted and downloads the configuration. For APs deployed on floor-2 on VLAN40, the controller IP address is provided through the DHCP option 191.

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 campus, or 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, we will create a user defined RF Domain and both the Wireless Controllers and all the Access Points will be part of this RF-Domain. The RF Domain will define regional and regulatory information as well as location and contact information.

For this configuration step a user defined RF Domains will be created:

1. A user defined RF Domain named corp will be created with the following parameters:
   a) The Country Code will be set to IN
   b) The Location will be set to BangaloreIN
   c) The Time Zone will be set to Asia/Calcutta
   d) The Contact will be set to sukhdeep@corp.local.

The user defined RF Domain corp will be manually assigned to each Wireless Controller using Device configuration. The corp RF Domain will be automatically assigned to Access Points using Auto-Provisioning Policies.

Command Line Interface

Use the following procedure to create a user defined RF Domain for the Wireless Controllers and Access Points using the Command Line Interface:

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

   rfs7000-81C20E(config)# rf-domain corp
   rfs7000-81C20E(config-rf-domain-corp)# country-code in
   rfs7000-81C20E(config-rf-domain-corp)# location BangaloreIN
   rfs7000-81C20E(config-rf-domain-corp)# timezone Asia/Calcutta
   rfs7000-81C20E(config-rf-domain-corp)# contact sukhdeep@corp.local
   rfs7000-81C20E(config-rf-domain-corp)# exit
2  Commit and Save the changes

rfs7000-81C20E(config)# commit write

**GUI configuration**

Use the following procedure to create a user defined RF Domain for the Wireless Controllers and Access Points using the Graphical User Interface:

1  Select Configuration → RF-Domains → Add
2 Enter the RF Domain name *corporate* then enter the Location and Contact information. Select a Time Zone and Country Code then click OK and Exit

<table>
<thead>
<tr>
<th>RF Domain</th>
<th>corp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Configuration</td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td></td>
</tr>
<tr>
<td>Contact</td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td></td>
</tr>
<tr>
<td>VLAN for Control Traffic</td>
<td></td>
</tr>
<tr>
<td>Smart RF</td>
<td></td>
</tr>
<tr>
<td>SMART RF Policy</td>
<td></td>
</tr>
<tr>
<td>Override Channel List 2.4 GHz</td>
<td></td>
</tr>
</tbody>
</table>

3 *Commit* and *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 Access Points will be assigned to a user defined Management policy. Depending on the management strategy, multiple Management Policies may be used for controllers or access points, or for a group of devices, as per need.

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

1. A user defined Management Policy named corp-mgmt-policy will be created to manage the Wireless Controllers in the data center with the following parameters:

   a) An administrative user account admin with the password hellomoto will be created and assigned to the Superuser role.

   b) HTTP will be disabled and HTTPS and SSHv2 secure management interfaces will be enabled.

The user defined Management Policies will be assigned to the Wireless Controllers and Access Points using user defined device Profiles.
Command Line Interface

Use the following procedure to create a user defined Management Policies for the Wireless Controllers and the Access Points using the Command Line Interface:

1. Create the user defined Management Policy for the Wireless Controllers in the data center named corp-mgmt-policy and define a admin user account and password with an assigned role and access permissions. Also create a Guest User admin guestadmin for creating guest user accounts. In addition disable HTTP and enable the secure HTTPS and SSHv2 management interfaces.

   ```
   rfs7000-81C20E(config)# management-policy corp-mgmt-policy
   rfs7000-81C20E(config-management-policy-corp-mgmt-policy)# user admin password 0 hellomoto role superuser access all
   rfs7000-81C20E(config-management-policy-corp-mgmt-policy)# user guestadmin password 0 hellomoto role web-user-admin
   rfs7000-81C20E(config-management-policy-corp-mgmt-policy)# no http server
   rfs7000-81C20E(config-management-policy-corp-mgmt-policy)# ssh
   rfs7000-81C20E(config-management-policy-corp-mgmt-policy)# https server
   rfs7000-81C20E(config-management-policy-corp-mgmt-policy)# exit
   ```

2. Commit and save the changes:

   ```
   rfs7000-81C20E(config)# commit write
   [OK]
   ```

Graphical User Interface

Use the following procedure to create a user defined Management Policies for the Wireless Controllers in the data center and the Access Points using the GUI:

1. Select Configuration → Management → Add
2 Enter the management policy name `corp-mgmt-policy` and click `Continue`:

<table>
<thead>
<tr>
<th>User Name</th>
<th>Access Type</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3 Select Administrators → Add:

<table>
<thead>
<tr>
<th>User Name</th>
<th>Access Type</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Type to search in tables: [Search Input]

Add | Edit | Delete | Exit
Enter the User Name \textit{admin} and Password \textit{hellomoto}. Select the Role \textit{Superuser}. Enable all access types. Click \textit{OK} and \textit{Exit}:

To create the guestadmin user to create guest accounts, click \textit{Add}. Enter the User Name \textit{guestadmin} and Password \textit{hellomoto}. Select the Role \textit{Web User}. Enable \textit{Web UI} access type. Click \textit{OK} and \textit{Exit}:
Select the Access Control Tab. Disable Http, Enable SSHv2 and HTTPS secure management interfaces. Click OK and Exit:

Commit and Save the changes:
2.3 Smart-RF

Smart RF (Self Monitoring At Run Time RF Management) helps in deployment planning by assigning the most appropriate channel and power to each radio on the managed access points. It does so while considering the site and application requirements, configured using the Smart-RF policies. It also monitors the RF environment at run time and adjusts the channel and power in response to dynamic changes to the RF environment, like coverage holes, new sources of interference and new neighboring access points. This ensures better coverage, more reliable wireless network and in turn better wireless client performance. The key features provided by Smart RF are:

1) **Neighbor recovery**: Defends against loss of coverage due to a sudden AP Failure.

2) **Coverage Hole**: Increase AP power if a client experiences reduced coverage.

3) **Interference recovery**: Change the operating channel if there is increased interference due to neighboring access points, or an external interference source like Bluetooth and microwave.

For this configuration step a Smart-RF will be created and assigned to an RF-Domain so that the wireless network can adjust to dynamic changes to the RF-environment.

1) Smart-RF policy named `corp-smart-rf` is created with the following parameters:
   
   a) Ensure the required Smart-RF features are enabled, like Interference recovery, Coverage Hole recovery, neighbor recovery.

   b) Edit the Smart-RF parameters like the channels

   c) Assign the Smart-RF policy created to the RF-Domain `corp`.

**Command Line Interface**

Use the following procedure to create a Smart RF Policy for the Wireless Infrastructure using the Command Line Interface:

1. **Create a Smart-RF policy corp-smart-rf. Enable the policy. Set the maximum assignable power during power assignment to 15 dBm. Assign the channels to be assigned during channel assignment to channels 1, 6 and 11 in the 2.4 GHz band and channels 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 161 and 165.**

   
   ```bash
   rfs7000-81C20E(config)# smart-rf-policy corp-smart-rf
   rfs7000-81C20E(config-smart-rf-policy-test)# assignable-power 5GHz max 15
   rfs7000-81C20E(config-smart-rf-policy-test)# assignable-power 2.4GHz max 15
   rfs7000-81C20E(config-smart-rf-policy-test)# channel-list 5GHz 36,40,44,48,52,56,60,64,149,153,157,161,165
   ```

2. **Assign the Smart-RF Policy corp-smart-rf to the RF-Domain corp:**

   ```bash
   rfs7000-81C20E(config)# rf-domain corp
   ```
rfs7000-81C20E(config- rf-domain-corp)# use smart-rf-policy corp-smart-rf
rfs7000-81C20E(config- rf-domain-corp)# exit

3 **Commit and Save the changes:**

rfs7000-81C20E(config)# commit write
[ OK ]

**Graphical User Interface**

Use the following procedure to create a Smart RF Policy for the Wireless Infrastructure using the Graphical user interface:

1 **Select Configuration → Wireless → Smart-RF Policy. Click Add:**

![Graphical User Interface](image)

2 **Enter Smart-RF policy name corp-smart-rf. Enable Smart RF policy. In this example, we use the pre-defined sensitivity level Medium and ensure the features Interference Recovery, Coverage Hole recovery and Neighbor recovery are enabled. Click OK:**

![Smart RF Policy](image)
Restrict the maximum power assigned by Smart-RF to 15 dBM on both the 2.4 GHz and 5 GHz band. Select the subset of channels out of which Smart-RF should assign a channel to the various Access points. We set this to channel 1, 6 and 11 on the 2.4 GHz band and the channels 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165 on the 5 GHz band Click OK and Exit:

We will assign the smart RF Policy to the RF-Domain corp. Select Configuration → RF Domains. Select the RF-Domain corp and click Edit. Select the Smart RF policy corp-smart-rf. Click OK and Exit:

Commit and Save the changes:
2.4 Wireless Intrusion Prevention (WIPS)

The uncontrolled propagation of wireless signals introduces new vulnerabilities that did not exist in the wired world. For example, rogue access points and attempts to break into your network by malicious users, even without being inside the corporate boundaries. WiNG 5 supports Wireless Intrusion Prevention which uses a threat detection engine onboard the wireless controller and access points providing visibility into 38 different threats, which can be categorized as:

1. Rogue AP detection
2. Excessive threshold violations detect traffic injection floods.
3. MU Anomaly detection detects wireless clients performing suspicious activities.
4. AP Anomaly detects threats like impersonation attempts, illegal frame types

Apart from this, the Advanced WIPS module unlocks additional threat detection capabilities and a protocol analysis engine for more complete detection of threats. This is a licensed module and supported only on the wireless controllers.

For this configuration step, a WIPS Policy will be created to prevent the wireless network against malicious activities.

1) A Smart-RF policy named corp-wips is created with the following parameters:
   a) Enable Rogue AP detection.
   b) Enable events against various attacks.
   c) Assign the WISP policy corp-wips to the RF-Domain corp.

Command Line Interface

Use the following procedure to create a WIPS Policy for the Wireless Infrastructure using the Command Line Interface:

1. Create a WIPS policy corp-wips and enable Rogue AP Detection.
   rfs7000-81C20E(config)# wips-policy corp-wips
   rfs7000-81C20E(config-wips-policy-corp-wips)# ap-detection

2. Enable the excessive events, MU anomaly events and AP anomaly events. You can enable all the events together using the enable-all-events command:
   rfs7000-81C20E(config-wips-policy-corp-wips)# event enable-all-events
   rfs7000-81C20E(config-wips-policy-corp-wips)# exit

3. Assign the WIPS Policy corp-wips to the RF-Domain corp:
   rfs7000-81C20E(config)# rf-domain corp
   rfs7000-81C20E(config-rf-domain-corp)# user wips-policy corp-wips
   rfs7000-81C20E(config-rf-domain-corp)# exit
4. Save and Commit the changes:

```
rfs7000-81C20E(config)# commit write
[ OK ]
```

**Graphical User Interface**

Use the following procedure to create a WIPS Policy for the Wireless Infrastructure using the Graphical User Interface:

1. Select Configuration → Security → Intrusion Prevention → WIPS Policy. Click Add:

   ![WIPS Policy Configuration](image1)

2. Type the WIPS Policy name `corp-wips` and enable “Rogue AP Detection”. Click OK:

   ![WIPS Policy Details](image2)
3 Enable the WIPS Events → Excessive tab. And enable all the Excessive Events. Configure the time for which the wireless client should be blacklisted in case any event is triggered. Click OK:

4 Enable the WIPS Events → MU Anomaly tab. Enable all the U Anomaly Events. You can configure the time for which the wireless client should be blacklisted/filtered. Click OK:
5 Enable the WIPS Events → AP Anomaly tab. And enable all the AP Anomaly. Click OK and Exit:

6 Assign the WIPS Policy to the RF Domain corp. Select Configuration → RF Domains. Select the RF Domain corp, and click Edit. Select the WIPS Policy corp-wips. Click OK and Exit:

7 Commit and Save the changes:
2.5 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.

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 initially using the Configuration Wizard. 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.

For this configuration step two Wireless LANs will be created. One using the 802.1x authentication using an external AAA server and the other using captive portal authentication with the captive portal and the AAA server hosted on the controller:

1) A **AAA Policy** named `external-aaa` will be created using centralized AAA servers deployed in the data center.

2) An **802.11i** **EAP** Wireless LAN named **CORP-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) The users are assigned to the VLAN **100 & 110**, depending on the user identity. The VLAN is assigned by the AAA server.
   
   d) Use **Tunnel bridging mode**.

3) A **AAA Policy** named **onboard-aaa** will be created using onboard AAA server on the wireless controller.

4) Create a **Captive Portal policy** named **GUEST** that is assigned to the Captive portal Wireless LAN:
   
   a) Select the Captive Portal **Server mode** as **centralized-controller**.
   
   b) Configure the Captive portal **server host** as `corp.local`. Please note that `corp.local` is a dummy FQDN. The AP will intercept it and provide the ip address of the controller. Ensure that the DNS server is provided by the DHCP server, and it is not on the same VLAN as the client, VLAN 200 in this case.
   
   c) Select the AAA policy we created earlier, **onboard-aaa**.
   
   d) Enable secure HTTP mode for communication.
   
   e) Assign the captive portal policy **GUEST** on the controller.
   
   f)
5) Create a Captive Portal Wireless LAN named GUEST with the following parameters:
   a) The Wireless LAN uses None authentication and encryption.
   b) Enable Captive Portal Policy and select the GUEST captive portal policy.
   c) The users on this Wireless LAN are assigned to the guest VLAN 200.
   d) Tunnel bridging mode is selected.

The CORP-DOT1X and GUEST Wireless LANs will be assigned to the AP650 Access Point radios using the user defined Profile named corp-ap650.

**Command Line Interface**

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

1. Create a AAA policy named external-aaa for the 802.1x EAP Wireless LAN:

   ```
   rfs7000-81C20E(config)# aaa-policy external-aaa
   ```

2. Create one or more Authentication server entries. In this example centralized Authentication servers 172.16.10.20 and 172.16.10.21 using proxy mode proxy-through-controller have been defined

   ```
   rfs7000-81C20E(config-aaa-policy-external-aaa)# authentication server 1 host 172.16.10.20 secret hellomoto
   rfs7000-81C20E(config-aaa-policy-external-aaa)# authentication server 2 host 172.16.10.21 secret hellomoto
   ```

3. Create a Wireless LAN CORP-DOT1X. Set the Encryption to CCMP, Authentication to EAP then assign the AAA Server Policy named external-aaa. Enable Tunnel bridging then assign the local VLAN 100 and VLAN 110:

   ```
   rfs7000-81C20E(config)# wlan CORP-DOT1X
   rfs7000-81C20E(config-wlan-CORP-DOT1X)# encryption-type ccmp
   rfs7000-81C20E(config-wlan-CORP-DOT1X)# authentication-type eap
   rfs7000-81C20E(config-wlan-CORP-DOT1X)# use aaa-policy external-aaa
   rfs7000-81C20E(config-wlan-CORP-DOT1X)# bridging-mode tunnel
   rfs7000-81C20E(config-wlan-CORP-DOT1X)# vlan-pool-member 100
   rfs7000-81C20E(config-wlan-CORP-DOT1X)# vlan-pool-member 110
   rfs7000-81C20E(config-wlan-CORP-DOT1X)# radius vlan-assignment
   rfs7000-81C20E(config-wlan-CORP-DOT1X)# exit
   ```

4. Create a AAA policy named onboard-aaa to be used with the captive portal Wireless LAN:

   ```
   rfs7000-81C20E(config)# aaa-policy onboard-aaa
   rfs7000-81C20E(config-aaa-policy-onboard-aaa)# authentication server 1 onboard controller
   ```
Create a Captive portal policy GUEST. Select the Captive portal server mode as \textit{centralized-controller}. Specify the Host as corp.local. Select the AAA policy \textit{onboard-aaa} that we created in the previous step:

```
rfs7000-81C20E(config)# captive-portal GUEST
rfs7000-81C20E(config-captive-portal-GUEST)# server mode centralized-controller
rfs7000-81C20E(config-captive-portal-GUEST)# server host corp.local
rfs7000-81C20E(config-captive-portal-GUEST)# use aaa-policy onboard-aaa
rfs7000-81C20E(config-captive-portal-GUEST)# connection-mode https
rfs7000-81C20E(config-captive-portal-GUEST)# exit
```

Create a captive portal Wireless LAN GUEST, with Encryption and Authentication as \textit{None}. Select the bridging mode \textit{Tunnel} and VLAN 200 and use the captive portal policy GUEST:

```
rfs7000-81C20E(config)# wlan GUEST
rfs7000-81C20E(config-wlan-GUEST)# ssid GUEST
rfs7000-81C20E(config-wlan-GUEST)# vlan 200
rfs7000-81C20E(config-wlan-GUEST)# bridging-mode tunnel
rfs7000-81C20E(config-wlan-GUEST)# encryption-type none
rfs7000-81C20E(config-wlan-GUEST)# authentication-type none
rfs7000-81C20E(config-wlan-GUEST)# captive-portal-enforcement
rfs7000-81C20E(config-wlan-GUEST)# use captive-portal GUEST
rfs7000-81C20E(config-wlan-GUEST)# exit
```

7. Commit and Save the changes

```
rfs7000-81C20E(config)# profile rfs7000 corp-rfs7000
rfs7000-81C20E(config-profile-corp-rfs7000)# use captive-portal server GUEST
rfs7000-81C20E(config-profile-corp-rfs7000)# exit
```

8. Commit and Save the changes

```
rfs7000-1(config)# commit write
[OK]
```
**Graphical User Interface**

Use the following procedure to create 802.11i Wireless LANs using the Graphical User Interface:

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

![Graphical User Interface screenshot]

2. **Enter the name external-aaa then click Continue**

![Add AAA Policy screenshot]
3 Select Radius Authentication tab. Click Add:

Set the Server Id to 1. Select the Server Type to Host and enter the ip address of the external AAA server 172.16.10.20 and the shared secret hellomoto. Select the Proxy Mode to Through Wireless Controller. Click OK then Exit
Click Add. Set the Server Id to 2 then enter the IP Address of the secondary AAA server 172.16.10.21. Set the Server Type to Host then enter the RADIUS Shared Secret, *hellomoto*. Set the Request Proxy Mode to *Through Wireless Controller*. Click OK and Exit.

Two RADIUS Authentication server entries have now been defined in the AAA Server Policy named *external-aaa*. Click Exit.
Select Configuration → Wireless → Wireless LANs → Add:

Enter the WLAN and SSID name as **CORP-DOT1X** and set the Bridging Mode to **Tunnel**. Enter the **VLAN ID 100** and select **Allow Radius Override**. Click OK and Exit. In this example, the users connected to the **Wireless LAN CORP-DOT1X** will be mapped to **VLAN 100 or VLAN 110**, as assigned by the radius server:
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.

Select Configuration → Wireless → AAA Policy → Add. Enter the name onboard-aaa and click Continue:
11 Select Radius Authentication tab. Click Add:

![Image of AAA Policy screen]

12 Set the Server Id to 1 then set the Server Type to onboard-controller. Click OK then Exit

![Image of Authentication Server settings]

To create the Captive portal policy, Select Configuration → Services → Captive Portals. Click Add. In the Captive Portal Policy field enter GUEST and set the Captive Portal Server Mode to Centralized Controller. Select Captive Portal Server field enter corp.local, which is a dummy fqdn. Select the AAA Policy named onboard-aaa. Click OK and Exit.

To create the captive portal wireless LAN, Select Configuration → Wireless → Wireless LANs → Add.
Enter the WLAN and SSID GUEST. Set the bridging mode to Tunnel and VLAN 200. Click OK. With None Encryption and Authentication. Select the bridging mode Tunnel and and use the captive portal policy GUEST.

Select Security. Set the Authentication Type to PSK/None then select the Encryption type Open. Select the Enforcement option Captive Portal Enable and select the captive portal policy GUEST. Click OK and Exit:
A Captive Portal Wireless LAN supporting RADIUS user authentication and centralized forwarding has now been created.

Assign the Captive Portal policy to the RFS7000 profile corp-rfs7000. Select Configuration → Profiles → corp-rfs7000. Click Edit. Select the Services Tab and enable the Captive Portal Policy Guest:

Commit and Save the changes:
2.6 Profiles

Profiles allow common configuration parameters and Policies to be assigned to groups of Wireless Controllers and Access Points. The configuration parameters within a Profile are based on the hardware model of the Wireless controller or access points. So a profile can only be assigned to a device belonging to the hardware model that it was created for.

Changes made to a Profile are automatically inherited by the devices using that profile allowing new services to be quickly deployed across the campus.

By default Controllers and Access Points are automatically assigned to a default 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 Campus deployment example, the Wireless Controllers and 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. Another user defined Profile will be created and automatically assigned to Access Points using Auto-Provisioning Policy.

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

4) A user defined RFS7000 device Profile named corp-rfs7000 will be created for the Wireless Controllers with the following parameters:
   a) Assign the user defined Management Policy corp-mgmt-policy created earlier.
   b) The ge1 port will be configured as a Trunk port with the Native VLAN ID 10.
   c) The Domain Name will be set to corp.local and the Name Server address set to 172.16.10.5.
   d) A NTP server 172.16.10.6 will be assigned.

5) A user defined AP650 device Profile named corp-ap650 will be created for the Access Points with the following parameters:
   a) Assign the user defined Management Policy corp-mgmt-policy, created earlier
   b) The ge1 port will be configured as an access port with the VLAN ID 30.
   c) The Wireless LAN named CORP-DOT1X will be assigned to both radio1 and radio2.
The user defined Controller Profile named corp-rfs7000 will be manually assigned to each RFS7000 Wireless Controller using Device configuration while the user defined AP Profile corp-ap650 and corp-ap650-floor2 will be automatically assigned to each Access Point as they are discovered and adopted using an Automatic Provisioning Policy. The Auto-Provisioning Policy will be assigned to the user defined Profile corp-rfs7000 in a later step.

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.

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.

Command Line Interface

Use the following procedure to create a user defined device Profiles for the Wireless Controllers and Access Points using the Command Line Interface:

1  Create a RFS7000 user defined Profile for the Wireless Controllers in the data center named corp-rfs7000

   rfs7000-81C20E(config)# profile rfs7000 corp-rfs7000

2  Assign the user defined Management policy named corp-mgmt-policy:

   rfs7000-81C20E(config-profile-corp-rfs7000)# use management-policy corp-mgmt-policy

3  Configure ge1 as a Trunk port and assign the tagged Native VLAN 10 and VLAN 10.

   rfs7000-81C20E(config-profile-corp-rfs7000)# interface ge1
   rfs7000-81C20E(config-profile-corp-rfs7000-if-up1)# description Uplink
   rfs7000-81C20E(config-profile-corp-rfs7000-if-up1)# switchport mode trunk
   rfs7000-81C20E(config-profile-corp-rfs7000-if-up1)# switchport trunk native vlan 10
   rfs7000-81C20E(config-profile-corp-rfs7000-if-up1)# switchport trunk allowed vlan 10,30,100,110,200
   rfs7000-81C20E(config-profile-corp-rfs7000-if-up1)# switchport trunk native tagged
   rfs7000-81C20E(config-profile-corp-rfs7000-if-up1)# exit
4 Assign a Domain Name, Name Server and NTP Server:

rfs7000-81C20E(config-profile-corp-rfs7000)# ip domain-name corp.local
rfs7000-81C20E(config-profile-corp-rfs7000)# ip name-server 172.16.10.5
rfs7000-81C20E(config-profile-corp-rfs7000)# ntp server 172.16.10.6

5 Create a user defined Profile for the AP650 Access Points named corp-ap650

rfs7000-81C20E(config)# profile ap650 corp-ap650
rfs7000-81C20E(config-profile-corp-ap650)#

6 Assign the user defined Management policy named corp-mgmt-policy

rfs7000-81C20E(config-profile-corp-ap650)# use management-policy corp-mgmt-policy

7 Assign the VLAN 30 to interface ge1:

rfs7000-81C20E(config-profile-corp-ap650)# interface ge1
rfs7000-81C20E(config-profile-corp-ap650-if-ge1)# description LAN
rfs7000-81C20E(config-profile-corp-ap650-if-ge1)# switchport access vlan 30
rfs7000-81C20E(config-profile-corp-ap650-if-ge1)# exit

9 Assign Wireless LANs to the 2.4 GHz radio1. In this example the Wireless LANs named CORP-DOT1X and GUEST are assigned to the 2.4 GHz radios:

rfs7000-81C20E(config-profile-corp-ap650)# interface radio 1
rfs7000-81C20E(config-profile-corp-ap650-if-radio1)# wlan CORP-DOT1X
rfs7000-81C20E(config-profile-corp-ap650-if-radio1)# wlan GUEST
rfs7000-81C20E(config-profile-corp-ap650-if-radio1)# exit

10 Assign Wireless LANs to the 5 GHz radio1. In this example only the Wireless LAN named CORP-DOT1X is assigned to the 5 GHz radios:

rfs7000-81C20E(config-profile-corp-ap650)# interface radio 2
rfs7000-81C20E(config-profile-corp-ap650-if-radio2)# wlan CORP-DOT1X
rfs7000-81C20E(config-profile-corp-ap650-if-radio2)# exit

11 Assign a Domain Name, Name Server and NTP Server:

rfs7000-81C20E(config-profile-corp-ap650)# ip domain-name corp.local
rfs7000-81C20E(config-profile-corp-ap650)# ip name-server 172.16.10.5
rfs7000-81C20E(config-profile-corp-ap650)# ntp server 172.16.10.6
rfs7000-81C20E(config-profile-corp-ap650)# exit
12 Verify the changes:

rfs7000-81C20E(config-profile-corp-ap650)# show context

profile ap650 corp-ap650
  ip name-server 172.16.10.5
  ip domain-name corp.local
  no autoinstall configuration
  no autoinstall firmware
  interface radio1
    wlan CORP-DOT1X bss 1 primary
    wlan GUEST bss 2 primary
  interface radio2
    wlan CORP-DOT1X bss 1 primary
  interface ge1
    description LAN
    switchport mode access
    switchport access vlan 30
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p

  use management-policy corp-mgmt-policy
  use firewall-policy default
  ntp server 172.16.10.6
  service pm sys-restart

13 Create a user defined Profile for the AP650 Access Points deployed in VLAN 40 named corp-ap650-floor2

rfs7000-81C20E(config)# profile ap650 corp-ap650-floor2
rfs7000-81C20E(config-profile-corp-ap650-floor2)#

14 Assign the user defined Management policy named corp-mgmt-policy

rfs7000-81C20E(config-profile-corp-ap650-floor2)# use management-policy corp-mgmt-policy

15 Create VLAN 40 with DHCP enabled:

rfs7000-81C20E(config-profile-corp-ap650-floor2)# interface vlan 40
rfs7000-81C20E(config-profile-corp-ap650-floor2-vlan40)# description VLAN40
rfs7000-81C20E(config-profile-corp-ap650-floor2-vlan40)# ip address dhcp
rfs7000-81C20E(config-profile-corp-ap650-floor2-vlan40)# ip dhcp client request options all
rfs7000-81C20E(config-profile-corp-ap650-floor2-vlan40)# exit
16 Assign the VLAN 40 to interface ge1:
```
rfs7000-81C20E(config-profile-corp-ap650-floor2)# interface ge1
rfs7000-81C20E(config-profile-corp-ap650-floor2-if-ge1)# description LAN
rfs7000-81C20E(config-profile-corp-ap650-floor2-if-ge1)# switchport access vlan 40
rfs7000-81C20E(config-profile-corp-ap650-floor2-if-ge1)# exit
```

17 Assign Wireless LANs to the 2.4 GHz radio1. In this example the Wireless LANs named CORP-DOT1X and GUEST are assigned to the 2.4 GHz radios:
```
rfs7000-81C20E(config-profile-corp-ap650-floor2)# interface radio 1
rfs7000-81C20E(config-profile-corp-ap650-floor2-if-radio1)# wlan CORP-DOT1X
rfs7000-81C20E(config-profile-corp-ap650-floor2-if-radio1)# wlan GUEST
rfs7000-81C20E(config-profile-corp-ap650-floor2-if-radio1)# exit
```

18 Assign Wireless LANs to the 5 GHz radio1. In this example only the Wireless LAN named CORP-DOT1X is assigned to the 5 GHz radios:
```
rfs7000-81C20E(config-profile-corp-ap650-floor2)# interface radio 2
rfs7000-81C20E(config-profile-corp-ap650-floor2-if-radio2)# wlan CORP-DOT1X
rfs7000-81C20E(config-profile-corp-ap650-floor2-if-radio2)# exit
```

19 Assign a Domain Name, Name Server and NTP Server:
```
rfs7000-81C20E(config-profile-corp-ap650-floor2)# ip domain-name corp.local
rfs7000-81C20E(config-profile-corp-ap650-floor2)# ip name-server 172.16.10.5
rfs7000-81C20E(config-profile-corp-ap650-floor2)# ntp server 172.16.10.6
```

20 Verify the changes:
```
rfs7000-81C20E(config-profile-corp-ap650-floor2)# show context
```

profile ap650 corp-ap650-floor2
  ip name-server 172.16.10.5
  ip domain-name corp.local
  no autoinstall configuration
  no autoinstall firmware
  interface radio1
    wlan CORP-DOT1X bss 1 primary
    wlan GUEST bss 2 primary
  interface radio2
    wlan CORP-DOT1X bss 1 primary
  interface ge1
    description LAN
    switchport mode access
    switchport access vlan 40
    ip dhcp trust
    qos trust dscp
    qos trust 802.1p
interface vlan40
description VLAN40
ip address dhcp
ip dhcp client request options all
use management-policy corp-mgmt-policy
use firewall-policy default
ntp server 172.16.10.6
service pm sys-restart

21 Commit and Save the changes:

rfs7000-81C20E(config-profile-corp-ap650-floor2)# exit
rfs7000-81C20E(config)# commit write
[ OK ]

Graphical User Interface

Use the following procedure to create a user defined device Profiles for the Wireless Controllers and the Access Points using the Graphical User Interface:

1 Select Configuration → Profiles → Add:
2 Type the Profile name corp-rfs7000 then set the Type to rfs7000. Under Network Time Protocol click Add Row then enter the NTP Server IP Address. Click OK:

3 Select Interface → Ethernet Ports → ge1 → Edit:
4. Enter a Description then set the Switching Mode to **Trunk**. Enter the Native VLAN and Allowed VLANs 10, 30, 100, 110 and 200. Select the option **Tag Native VLAN** then click OK and Exit.

5. Select Management → Settings. Assign the user defined Management Policy named corp-mgmt-policy then click OK:
Select Network → DNS. Assign the Domain Name then enter the Name Server IP address. Click OK then Exit.

A user defined Profile named corp-rfs7000 has now been created. Click Add to create a user defined Profile for the AP650 Access Points.
8 Type the Profile name corp-ap650 and set the Type to AP650. Click OK:

9 Select Interface → Ethernet Ports → ge1→ Edit:
10 Enter a Description **LAN** and enter the Native VLAN 30. Click OK and Exit

11 Select Interface → Radios → radio1 → Edit:
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 CORP-DOT1X and GUEST have been assigned to the 2.4 GHz radio:

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 CORP-DOT1X has been assigned to the 5 GHz radio:
Select Management → Settings. Assign the user defined Management Policy named corp-mgmt-policy and click OK:

A user defined Profile named corp-ap650 has now been created:
Click Add to create another user defined profile for AP650 on floor 2. Type the Profile name corp-ap650-floor2 and set the Type to ap650. Click OK:

Select Interface → Virtual Interfaces → Add. Enter VLAN 40. Select DHCP addressing and enable Use DHCP to obtain Gateway/DNS Servers. Click OK and Exit:
18 **Select Interface → Ethernet Ports → ge1 → Click Edit. Enter a Description and enter the Native VLAN 30. Click OK and Exit**

<table>
<thead>
<tr>
<th>Ethernet Ports</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>ge1</td>
</tr>
</tbody>
</table>

- **Properties**
  - **Description**: LAN
  - **Admin Status**: Enabled
  - **Speed**: Automatic
  - **Duplex**: Automatic
  - **CDP/LLDP**
    - **Class Discovery Protocol Receive**: Enabled
    - **Class Discovery Protocol Transmit**: Enabled
    - **Link Layer Discovery Protocol Receive**: Enabled

- **Switching Mode**
  - **Mode**: Access
  - **Native VLAN**: 40
  - **Tag Native VLAN**: (1 to 4094)
  - **Allowed VLANs**: (2, 4, 7-12, ...)

19 **Select Interface → Radios → radio1 → Edit:**

<table>
<thead>
<tr>
<th>Profile</th>
<th>corp-ap650-floor2</th>
<th>Type</th>
<th>AP650</th>
</tr>
</thead>
</table>

- **General**
- **Addition**
- **Interface**
  - **Ethernet Ports**
  - **Virtual Interfaces**
- **Radios**
  - **PPPoE**
  - **Network**
  - **Security**
  - **Critical Resources**
  - **Services**
  - **Management**
  - **Advanced**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Admin Status</th>
<th>RF Mode</th>
<th>Channel</th>
<th>Transmit Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>radio1</td>
<td>Radio</td>
<td>radio1</td>
<td>Enabled</td>
<td>2.4 GHz VLAN</td>
<td>smart</td>
<td>smart</td>
</tr>
<tr>
<td>radio2</td>
<td>Radio</td>
<td>radio2</td>
<td>Enabled</td>
<td>5 GHz VLAN</td>
<td>smart</td>
<td>smart</td>
</tr>
</tbody>
</table>
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 CORP-DOT1X and GUEST have been assigned to the 2.4 GHz radio:

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 CORP-DOT1X has been assigned to the 5 GHz radio:
22 Select Management → Settings. Assign the user defined Management Policy named corp-mgmt-policy and click OK:

![User interface showing Management Policy settings](image)

23 A user defined Profile named corp-ap650-floor2 has now been created. Save and Commit the changes:
2.7 Radius Server

For Guest users, the radius server is configured on the wireless controllers. The radius service is working in high availability mode on the two wireless controllers working in active-active clustering mode. The guest users are created by the Web Admin user, which could be done by any non-technical user like the receptionist, and they are synced between the two controllers.

1. Create a Radius Group Policy **guest-users** with the following parameters:
   a) Allowed Wireless LAN SSID of **GUEST**

2. Create a Guest user pool **guest-user-pool**. Users will be added to this pool later using the Web Admin:

3. Create a radius server policy **corp-radius-server** with the following parameters:
   a) The allowed radius users Pools of **guest-user-pool**

4. Apply the radius server policy **corp-radius-server** to the RFS7000 profile **corp-rfs7000**
   a) Select the user group **guest-user-pool**

2.7.1 Radius Server Policy:

**Command Line Interface**

Use the following procedure to create a radius server policy for the guest users using the command line interface:

1. **Create a radius group guest-users for the GUEST users:**

   rfs7000-1(config)# radius-group guest-users
   rfs7000-1(config-radius-group-guest-users)# guest
   rfs7000-1(config-radius-group-guest-users)# policy ssid GUEST
   rfs7000-1(config-radius-group-guest-users)# exit

2. **Create a radius users pool guest-user-pool. The users will be created later by the Web Admin using the Web Interface:**

   rfs7000-1(config)# radius-user-pool-policy guest-user-pool
   rfs7000-1(config-radius-user-pool-guest-user-pool)# exit

3. **Create a RADIUS Server Policy corp-radius-server. Assign the RADIUS User Pool named guest-user-pool:**

   rfs7000-1(config)# radius-server-policy corp-radius-server
   rfs7000-1(config-radius-server-policy-corp-radius-server)# use radius-user-pool-policy guest-user-pool
   rfs7000-1(config-radius-server-policy-corp-radius-server)# exit
4 Apply the radius server policy to the RFS7000 profile:

rfs7000-1(config)# profile rfs7000 corp-rfs7000
rfs7000-1(config-profile-corp-rfs7000)# user radius-server-policy corp-radius-server
rfs7000-1(config-profile-corp-rfs7000)# exit

5 Commit and Save the changes:

rfs7000-1(config)# commit write
[OK]

Graphical User Interface

Use the following procedure to create a radius server policy for the guest users using the graphical user interface:

1 Select Configuration → Services → RADIUS → Groups → Add:
In the RADIUS Group Policy name field enter guest-users. In the WLAN SSID name field GUEST and click the Add button. Click OK then Exit.

3 Select Radius → User Pools → Add:
4 In the User Pool field enter guest-user-pool then click Continue. Guest users will be created in the guest-user-pool using the Web Admin interface:

5 To Create a Radius Server Policy, select Radius → Server Policy → Add.
In the RADIUS Server Policy field enter corp-radius-server. Assign the RADIUS User Pool named guest-user-pool then click OK and Exit.

A RADIUS Server Policy named corp-radius-server has now been created. Apply this radius server policy to the RFS7000 profile. Select Configuration → Profiles → corp-rfs7000. Select the Services Tab and select the corp-radius-server policy created in the last step:
2.7.1 Guest User Creation

The Guest users can be created using the web interface by the Web User admin role. The Web Admin `guestadmin` was created in section 2.2 in the management policy `corp`.

**Graphical User Interface**

Use the following procedure to create a guest user using the graphical user interface:

1. Login using the user `guestadmin` and password `hellomoto`:

2. On the Guest User Configuration page, select the User Pool `eap-users-pool` and Click Create New User:
Enter username guestuser and password hellomoto. Select the user group guest-users and the Start date/time and the Expiry date/time.

Guest User Configuration

User Pool: guest-user-pool
Username: guestuser
Password: hellomoto
User Group: guest-users
Start Date/Time: 05/20/2012 05:21 AM
Expiry Date/Time: 05/25/2012 05:21 AM

Generate

Back  Print Voucher  Create User  Clear Fields
2.8 Role Based Access Control

Wired clients access the network through a fixed port and location which is usually protected by physical boundary. But this is not true for the wireless networks. So, there is a need to find out the identity of the wireless user and apply access policies based on his role within the organization, irrespective of the location from where it is accessing the wireless network. So, even though the Finance and Human Resource employees access the wireless network using a common ESSID, their access policies will depend on their identities.

The users can be grouped according to their role and the access policies are applied to this group. The user role can be identified based on one of the parameters like the device MAC address, Authentication type, Encryption type, user group or ESSID.

For this configuration step, the guest role is created and access restrictions are applied to this role:
1. A wireless client role guest-role is created for users who join the GUEST Wireless LAN.
2. An IP Firewall rule is created that prevents access to the data center network by the guest users.
3. The IP Firewall rule is attached to the guest-role in the Inbound direction.
4. The Guest role is applied to the access points profiles corp-ap650 and corp-ap650-floor2.

Command Line Interface

Use the following procedure to create a wireless client role for the guest users and apply access policies on this role using the Command Line Interface:

1. Create an IP Firewall Rule to block access to the 172.16.10.0/24 subnet from the Guest users. Deny all the other traffic:

   rfs7000-1(config)# ip access-list acl-guest
   rfs7000-1(config-ip-acl-allow-http)# deny ip 172.16.200.0/24 172.16.10.0/24 rule-precedence 10
   rfs7000-1(config-ip-acl-allow-http)# permit ip any any rule-precedence 20
   rfs7000-1(config-ip-acl-allow-http)# exit

2. Create a Role policy corp and create a wireless client role guest-role for users attached to the GUEST Wireless LAN. Apply the IP Firewall rule acl-guest to the guest-role in the Inbound direction:

   rfs7000-1(config)# role-policy corp
   rfs7000-1(config-role-policy-corp)# user-role guest-role precedence 1
   rfs7000-1(config-role-policy-corp)# ssid exact GUEST
   rfs7000-1(config-role-policy-corp)# use ip-access-list in acl-guest precedence 1
   rfs7000-1(config-role-policy-corp)# exit

3. Assign the role policy corp to the AP profiles:

   rfs7000-1(config)# profile ap650 corp-ap650
   rfs7000-1(config-profile-corp-ap650)# use role-policy corp
   rfs7000-1(config-profile-corp-ap650)# exit
   rfs7000-1(config)# profile ap650 corp-ap650-floor2
   rfs7000-1(config-profile-corp-ap650-floor2)# use role-policy corp
   rfs7000-1(config-profile-corp-ap650-floor2)# exit
rfs7000-1(config-profile-corp-ap650-floor2)# use role-policy corp
rfs7000-1(config-profile-corp-ap650-floor2)# exit

4 Commit and save the changes:

rfs7000-1(config)# commit write
[OK]

Graphical User Interface

Use the following procedure to create Role corp for guest users using the Management User Interface:

1 Create an IP Firewall Rule to block traffic to the 172.16.10.0/24 subnet from the GUEST VLAN. Select Configuration → Security → IP Firewall Rules → Click Add.
2 In the Firewall Rules field enter acl-guest and click Add Row. Create a rule to Deny access from the guest VLAN 172.16.200.0/24 to the management subnet 172.16.10.0/24:

3 Click Add Row. Create a rule to Permit all other traffic. Click Ok and Exit:
To create a Wireless Client Role, select Configuration → Security → Wireless Client Roles → Add:

5 Enter the role policy corp. Click Continue:
Enter the role name guest-role. Select the SSID configuration match condition to Exact and enter the value GUEST. Click OK:

<table>
<thead>
<tr>
<th>Role Policy Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Name</td>
</tr>
<tr>
<td>SSID Configuration</td>
</tr>
<tr>
<td>Group Configuration</td>
</tr>
<tr>
<td>Wireless Client Filter</td>
</tr>
<tr>
<td>Captive Portal Connection</td>
</tr>
<tr>
<td>Authentication Type</td>
</tr>
<tr>
<td>Encryption Type</td>
</tr>
</tbody>
</table>

Select the Firewall Rules and under the IP Inbound section, click Add Row. Select the IP Firewall rule acl-guest. Click OK and Exit:

<table>
<thead>
<tr>
<th>Role Policy Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Name</td>
</tr>
<tr>
<td>IP Inbound</td>
</tr>
<tr>
<td>MAC Inbound</td>
</tr>
<tr>
<td>IP Firewall Rules Name</td>
</tr>
<tr>
<td>MAC Firewall Rules Name</td>
</tr>
</tbody>
</table>

Select the Firewall Rules and under the IP Inbound section, click Add Row. Select the IP Firewall rule acl-guest. Click OK and Exit:
Assign the role policy to the user defined profile ap650-corp. Select Configuration → Profiles → corp-ap650 → Edit. Select Security tab and assign the corp Wireless Client Role Policy. Click OK and Exit:

Assign the role policy to the user defined profile ap650-corp-floor2. Select Configuration → Profiles → corp-ap650-floor2 → Edit. Select Security tab and assign the corp Wireless Client Role Policy. Click OK and Exit:

Save and Commit the changes:
2.9 Clustering

WiNG 5.x supports clustering (redundancy) to reduce the chances of disruption in the WLAN services in the event of a failure of a switch or an intermediate network failure by deploying more than one controller in Active-Active or Active-Standby mode. Clustering can be enabled between wireless controllers to provide seamless failover of access points and other services like Radius and DHCP redundancy.

Clusters are managed by a single management interface and configurations are synchronized between the cluster members. System wide events and statistics are available from any management interface.

**Smart Licensing:**

WiNG 5 supports smart license sharing between the wireless controllers in the cluster. The Access point licenses of all the controllers in the cluster are aggregated to get the combined license count of the cluster. In the event of failure of any one controller in the cluster, the license count on that controller is shared between other controllers in the cluster.

In this example configuration, 2 RFS7000 controllers are configured in an active-active clustering mode, and load balance the access points between each other. The number of license is equal to the number of access points and one does not need additional licenses for failover.

**Device Overrides**

In the previous step we defined a user defined Profiles which assigned common configuration parameters to the Wireless Controllers and 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.

2.9.1 Wireless Controller (Cluster Master)

In clustering mode, one of the controllers is elected (or designated) as a master controller, responsible for configuration sync amongst other members in the cluster. For this configuration step the Wireless Controller that is designated as the Cluster Master will be assigned the following Device Configuration:

1) The user defined Profile named *corp-rfs7000* will be assigned.

2) The user defined RF Domain named *corp* will be assigned.

3) The Hostname will be set to *rfs7000-1*.

4) A Virtual IP Interface for VLAN 10 will be created and the static IP address 172.16.10.10/11 assigned.

5) A default route pointing to 172.16.10.1 will be defined.

6) The cluster name will be set to *corp*. 
7) The cluster priority will be set to **255** (highest value becomes the master).

8) A **Level 1 IP MINT Link** will be defined pointing to the Cluster Members IP address **172.16.10.11**.

**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 corp and user defined Profile named corp\rfs7000**
   
   ```
   rfs7000-81C20E(config)# self
   rfs7000-81C20E(config-device-00-15-70-81-C2-0E)# use profile corp\rfs7000
   rfs7000-81C20E(config-device-00-15-70-81-C2-0E)# use rf-domain corp
   ```

2. **Define a Hostname for the device. Note in this example the hostname rfs7000-1 is assigned:**
   
   ```
   rfs7000-81C20E(config-device-00-15-70-81-C2-0E)# hostname rfs7000-1
   ```

3. **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 10 has been created and the static IP address 172.16.10.10/24 assigned:**
   
   ```
   rfs7000-81C20E(config-device-00-15-70-81-C2-0E)# interface vlan 10
   rfs7000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan10)# description Management\VLAN
   rfs7000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan10)# ip address 172.16.10.10/24
   rfs7000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan10)# exit
   ```

4. **Create a Virtual IP Interface for the Guest VLAN 200 and assign a static IP address. Note in this example a Virtual IP interface for VLAN 200 has been created and the static IP address 172.16.200.10/24 assigned**
   
   ```
   rfs7000-81C20E(config-device-00-15-70-81-C2-0E)# interface vlan 200
   rfs7000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan200)# description Guest\VLAN
   rfs7000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan200)# ip address 172.16.200.10/24
   rfs7000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan200)# exit
   ```

5. **Assign a default gateway. Note in this example the default gateway for VLAN 10 is 172.16.10.1**
   
   ```
   rfs7000-81C20E(config-device-00-15-70-81-C2-0E)# ip route 0.0.0.0/0 172.16.10.1
   ```
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 corp and the Cluster Members IP address is 172.16.10.11. In addition the MINT link level between the cluster peers is set to Level 1:

rfs7000-81C20E(config-device-00-15-70-81-C2-0E)# cluster name corp
rfs7000-81C20E(config-device-00-15-70-81-C2-0E)# cluster member ip 172.16.10.11 level 1
rfs7000-81C20E(config-device-00-15-70-81-C2-0E)# cluster master-priority 255
rfs7000-81C20E(config-device-00-15-70-81-C2-0E)# exit

6  **Commit and Save the changes**

rfs7000-81C20E(config)# commit write

[ OK ]

**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 → rfs7000-<mac> → Edit**
2. Set the System Name to `rfs7000-1` then assign the user defined RF Domain `corp`.

3. SelectProfile Overrides → Interface → Virtual Interfaces. Click Add to create a new interface for the Native VLAN 20.
4. Enter the VLAN ID of VLAN 10, Description and Primary IP Address 172.16.10.10/24. Click OK and Exit:

5. Select Profile Overrides → Network → Routing → Static Routes. Click Add Row. In the network address field, enter 0.0.0.0/0 and in the gateway field, enter the default gateway of 172.16.10.1 for the VLAN 10:
Select Profile Overrides → Cluster. Verify the cluster mode is Active. Enter the Cluster Name corpus and set the Master Priority to 255. Under Cluster Member click Add Row. Enter the IP Address assigned to the Cluster Member, 172.16.10.11. Verify the Routing Level is 1. Click OK and Exit:

The Device configuration for the Cluster Master switch is now completed. Commit and Save the changes:
2.9.2 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 user defined Profile named corp-rfs7000 will be assigned.
2) The user defined RF Domain corp will be assigned.
3) The Hostname will be set to rfs7000-2.
4) A Virtual IP Interface for VLAN 10 will be created and the IP address 1972.16.20.11/24 assigned.
5) A default route pointing to 172.16.10.1 will be defined.
6) The cluster name will be set to corp.
7) The cluster priority will be set to 100 (lower than the Cluster Master).
8) Configure the cluster member, which is Cluster Masters IP address 172.16.10.10. Specify Level 1 IP MINT Link.

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.

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:

```
rfs7000-1(config)# rfs7000 5C-0E-8B-17-C8-73
```

2 Assign the user defined RF Domain named corp and user defined Profile named corp-rfs7000

```
rfs7000-1(config-device-5C-0E-8B-17-C8-73)# use profile corp-rfs7000
```
rfs7000-1(config-device-5C-0E-8B-17-C8-73)# use rf-domain corp

3 Define a Hostname for the device. Note in this example the hostname rfs7000-2 is assigned

rfs7000-1(config-device-5C-0E-8B-17-C8-73)# hostname rfs7000-2

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 10 has been created and the static IP address 172.16.10.11/24 assigned

rfs7000-1(config-device-5C-0E-8B-17-C8-73)# interface vlan 10
rfs7000-1(config-device-5C-0E-8B-17-C8-73-if-vlan10)# description Management VLAN
rfs7000-1(config-device-5C-0E-8B-17-C8-73-if-vlan10)# ip address 172.16.10.11/24
rfs7000-1(config-device-5C-0E-8B-17-C8-73-if-vlan10)# exit

5 Create a Virtual IP Interface for the Guest VLAN 200 and assign a static IP address. Note in this example a Virtual IP interface for VLAN 200 has been created and the static IP address 172.16.200.11/24 assigned

rfs7000-1(config-device-5C-0E-8B-17-C8-73)# interface vlan 200
rfs7000-1(config-device-5C-0E-8B-17-C8-73-if-vlan200)# description Guest VLAN
rfs7000-1(config-device-5C-0E-8B-17-C8-73-if-vlan200)# ip address 172.16.200.11/24
rfs7000-1(config-device-5C-0E-8B-17-C8-73-if-vlan200)# exit

6 Assign a default gateway of 172.16.10.1 on VLAN 10:

rfs7000-1(config-device-5C-0E-8B-17-C8-73)# ip route 0.0.0.0/0 172.16.10.1

7 Specify the Cluster Name corp, Cluster Member IP Address, 172.16.10.10 and set the Cluster Priority to 100. The MINT link level between the cluster peers is set to Level 1:

rfs7000-1(config-device-5C-0E-8B-17-C8-73)# cluster name corp
rfs7000-1(config-device-5C-0E-8B-17-C8-73)# cluster member ip 172.16.10.10 level 1
rfs7000-1(config-device-5C-0E-8B-17-C8-73)# cluster master-priority 100

7 Verify the changes:

rfs7000-1(config-device-5C-0E-8B-17-C8-73)# show context

rfs7000 5C-0E-8B-17-C8-73
use profile corp-rfs7000
use rf-domain corp
hostname rfs7000-2
ip default-gateway 172.16.10.1
interface vlan10
description Management
8 Exit the Profile configuration then Commit and Save the changes:

rfs7000-1(config-device-5C-0E-88-17-C8-73)# exit
rfs7000-1(config)# commit write
[ OK ]

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
Enter the Cluster Members Device MAC address and set the Type to RFS7000. Set the System Name to rfs7000-2 then assign the user defined RF Domain named corp and the Profile named corp-rfs7000. Click OK.

Select Profile Overrides → Interface → Virtual Interfaces → Add:
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 172.16.10.11/24.

Select Profile Overrides → Network → Routing → Static Routes. Click Add Row. In the Network Address field enter 0.0.0.0/0 and in the Gateway field enter the IP address of the default gateway, 172.16.10.1 on VLAN 10. Click OK:
Select Profile Overrides → Cluster. In the Cluster Name field enter corp then set the Master Priority to 100. Under Cluster Member click Add Row. Enter the IP Address assigned to the Cluster Master 172.16.10.10. Set the Routing Level to 1:

The Device configuration for the Cluster Member switch is now completed:
2.10 Auto Provisioning Policies

When an access point is adopted by a Wireless Controller, the controller determines the configuration to be applied to the access point. Since multiple configuration policies are supported the wireless controller needs a way of determining which of the multiple configuration policies should be used for the given access point. Auto Provisioning Policies provide a way to determine a configuration policy to be used for an access point based on some of its properties, like it’s VLAN, IP or MAC address, etc.

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

Auto 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 campus deployments, these rules are typically based on the VLAN or 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 site.

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

1) An Automatic Provisioning Policy named corp will be created and assigned to the RFS7000 user defined Profile named corp-rfs7000.

   i. An AP650 rule assigning the user defined RF Domain named corp and user defined Profile named corp-ap650 will be defined with a match based on the source VLAN 30.

At least one Automatic Provisioning Policy rule will be required for each campus deployment. As rules are Access Point model dependent, multiple rules may be required if multiple Access Point models are deployed. For example if both AP621 and AP650 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 corp with rule to adopt AP650 access points connected to the controller on VLAN 30. Assign the user defined Profile named corp-ap650 and RF Domain corp:

   ```
   rfs7000-1(config)# auto-provisioning-policy corp
   rfs7000-1(config-auto-provisioning-policy-corp)# adopt ap650 precedence 1 profile corp-ap650 rf-domain corp vlan 30
   ```

2. Add a rule to adopt AP650 access points deployed on the VLAN 40, and assigned ip address in the subnet 172.16.40.0/24. Assign the user defined Profile named corp-ap650-floor2 and RF Domain corp:

   ```
   rfs7000-1(config-auto-provisioning-policy-corp)# adopt ap650 precedence 2 profile corp-ap650-floor2 rf-domain corp ip 172.16.40.0/24
   rfs7000-1(config-auto-provisioning-policy-corp)# exit
   ```

3. Access the RFS7000 user defined Profile named corp-rfs7000 and assign the Automatic Provisioning Policy named corp:

   ```
   rfs7000-1(config)# profile rfs7000 corp-rfs7000
   rfs7000-1(config-profile-corp-rfs7000)# use auto-provisioning-policy corp
   rfs7000-1(config-profile-corp-rfs7000)# exit
   ```

4. Save and Commit the changes:

   ```
   rfs7000-1(config)# commit write
   [ OK ]
   ```
Graphical User Interface

Use the following procedure to create and assign Auto-Provisioning Policy and rules using the Graphical User Interface:

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

   Auto-Provisioning
   
   Auto-Provisioning Policy  Admin if No Rules Match

   2. Enter the Auto-Provisioning Policy name corp and click Continue. Then click Add.
Set the Rule Precedence to 1 then set the Device Type to AP650. Set the Match Type to VLAN and enter the VLAN 30 to which the Access Points are connected to. Assign the RF Domain named corp and the Profile named corp-ap650. Click OK then Exit:

Set the Rule Precedence to 2 then set the Device Type to AP650, the Match Type to IP Address and enter subnet 172.16.40.0/24 on which the Access Points are deployed. Assign the RF Domain named corp and the Profile named corp-ap650-floor2. Click OK then Exit:
An Automatic Provisioning Policy with two rules has now been defined. Assign this to the RFS7000 profile corp-rfs7000. Select Configuration → Profiles → corp-rfs7000 → Edit. Select Adoption and assign the auto-provisioning policy named corp. Click OK and Exit:

The Automatic Provisioning Policy named corp has now been assigned to the RFS7000 user defined Profile named corp-rfs7000. Commit and Save the changes:
2.11 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 RFS7000s in the cluster will establish MINT links, elect a master then become active. On any subsequent configuration change, the configuration on the master controller will be automatically synchronized with the cluster member’s configuration.

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:
   ```
   rfs7000-1# 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:
   ```
   rfs7000-1# copy usb1:cluster.cfg startup-config
   ```

3. Reload the Cluster Member controller:
   ```
   rfs7000-17C873# reload
   The system will be rebooted, do you want to continue? [y/n]: y
   Save current configuration? {yes/no/display unsaved/cancel 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 rfs7000-1 with the priority 255 has become the Cluster Master and rfs7000-2 with the priority 100 has become a Cluster Member:
   ```
   rfs7000-1# show cluster members
   -----------------------------------------------------------------------------------------------
   HOSTNAME  MEMBER-ID   MAC MASTER   STATE STATUS LAST-SEEN
   rfs7000-1  70.81.C2.0E  00-15-70-81-C2-0E   True active up 00:10:12 ago
   rfs7000-2  0B.17.C8.73  5C-0E-8B-17-C8-73  False 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
   ```
   rfs7000-1# show cluster members detail
   ```
Use the show cluster status command to display Cluster Runtime Information. This will display the overall Cluster State, License Pooling and Adoption Capacity information:

```
rfs7000-1# show cluster status
Cluster Runtime Information
Protocol version : 1
Cluster state : active
AP license : 128
AAP license : 256
AP count : 0
AAP count : 0
Max AP adoption capacity : 2048
Number of connected member(s): 1
```

### 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: 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:

```
rfs7000-1# show adoption info

HOST-NAME        MAC         TYPE    MODEL
ap650-C78704     00-15-70-C7-87-04  ap650   AP-0650-66040-US
ap650-316428     00-23-68-31-64-28  ap650   AP-0650-66040-US
ap650-860F18     00-23-68-86-0F-18  ap650   AP-0650-66040-US

Total number of APs displayed: 3
```

At least one Automatic Provisioning Policy rule will be required for each site. If different policies need to be configured on group of access points, then multiple auto provisioning policies will be needed. Also, 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 AP650 Access Points are deployed, two Automatic Provisioning Policy rules will be required.

Issue the `show adoption status` command to view detailed adoption information about the Access Points adopted by the Wireless Controllers. 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**:

```
rfs7000-1# show adoption status

HOST-NAME        VERSION   CFG STAT  ADOPTED-BY   LAST-ADOPTION   UPTIME
ap650-C78704     5.3.1.0-009R configured  rfs7000-1 2012-05-25 11:12:30 0 days 00:27:03
ap650-316428     5.3.1.0-009R configured  rfs7000-2 2012-05-25 11:12:15 0 days 00:27:03
ap650-860F18     5.3.1.0-009R configured  rfs7000-2 2012-05-25 11:12:15 0 days 00:27:03

Total number of APs displayed: 3
```

You can quickly filter the output of a command using `grep` to look for specific information. For example issuing the `show adoption status | grep rfs7000-1` command will display all the Access Points adopted by RFS7000 `rfs7000-1`

3.2 Verifying RF Domains

3.2.1 `show noc device`
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.

```
rfs7000-1# show noc device
```

<table>
<thead>
<tr>
<th>MAC</th>
<th>HOST-NAME</th>
<th>TYPE</th>
<th>CLUSTER</th>
<th>RF-DOMAIN</th>
<th>ADOPTED-BY</th>
<th>ONLINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-15-70-81-C2-0E</td>
<td>rfs7000-1</td>
<td>rfs7000</td>
<td>corp</td>
<td>corp</td>
<td></td>
<td>online</td>
</tr>
<tr>
<td>5C-0E-8B-17-C8-73</td>
<td>rfs7000-2</td>
<td>rfs7000</td>
<td>corp</td>
<td>corp</td>
<td>00-15-70-81-C2-0E</td>
<td>online</td>
</tr>
<tr>
<td>00-15-70-C7-87-04</td>
<td>ap650-C78704</td>
<td>ap650</td>
<td>corp</td>
<td></td>
<td>5C-0E-8B-17-C8-73</td>
<td>online</td>
</tr>
<tr>
<td>00-23-68-31-64-28</td>
<td>ap650-316428</td>
<td>ap650</td>
<td>corp</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00-23-68-86-0F-18</td>
<td>ap650-860F18</td>
<td>ap650</td>
<td>corp</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total number of clients displayed: 5

### 3.2.2 show noc domain managers

Issue the **show noc domain managers** command to validate the controller serving as the RF Domain Manager for each of the defined RF Domains.

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

<table>
<thead>
<tr>
<th>RF-DOMAIN</th>
<th>MANAGER</th>
<th>HOST-NAME</th>
<th>APS</th>
<th>CLIENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>corp</td>
<td>00-15-70-81-C2-0E</td>
<td>rfs7000-1</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

Total number of RF-domain displayed: 1

### 3.3 Verifying MINT

Issue the **show mint links** command on each of the Wireless Controllers to view the established VLAN and IP based MINT links. One Level 1 IP based MINT link will be present on each Wireless Controller for the cluster, one Level 1 VLAN MINT link on VLAN 30 and one Level 1 IP based MINT link will be present to each L3 adopted access point. In the example below each Layer 2 adopted AP (in VLAN 30) will have a Level 1 MINT link on VLAN 30 while two Level 1 IP based MINT links have been established to the 2 wireless controllers **rfs7000-1** and **rfs7000-2** from the L3 adopted access points (in VLAN 40).

```
rfs7000-1# show mint links on rfs7000-1
4 mint links on 70.81.C2.0E:
link ip-172.16.10.11:24576 at level 1, 1 adjacencies
link ip-172.16.40.109:24576 at level 1, 1 adjacencies
link ip-172.16.40.110:24576 at level 1, 1 adjacencies
link vlan-30 at level 1, 2 adjacencies, DIS 70.81.C2.0E (self)
```

```
rfs7000-1# show mint links on rfs7000-2
4 mint links on 70.81.C2.0E:
link ip-172.16.10.10:24576 at level 1, 1 adjacencies
link ip-172.16.40.109:24576 at level 1, 1 adjacencies
link ip-172.16.40.110:24576 at level 1, 1 adjacencies
link vlan-30 at level 1, 2 adjacencies, DIS 70.81.C2.0E (self)
```

rfs7000-1# show mint links on rfs7000-1
4 mint links on 70.81.C2.0E:
link ip-172.16.10.11:24576 at level 1, 1 adjacencies
link ip-172.16.40.109:24576 at level 1, 1 adjacencies
link ip-172.16.40.110:24576 at level 1, 1 adjacencies
link vlan-30 at level 1, 2 adjacencies, DIS 70.81.C2.0E (self)
3.4 Verifying Smart-RF

To verify the channels assigned to the access points, use the command `show smart-rf radio`:

### 3.4.1 show smart-rf radio

Rfs7000-1# show smart-rf radio

<table>
<thead>
<tr>
<th>AP</th>
<th>RADIO-MAC</th>
<th>TYPE</th>
<th>STATE</th>
<th>CHANNEL</th>
<th>POWER</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap650-C78704</td>
<td>00-15-70-30-88-F0</td>
<td>11an</td>
<td>normal</td>
<td>149+</td>
<td>15</td>
</tr>
<tr>
<td>ap650-C78704</td>
<td>00-15-70-30-8C-30</td>
<td>11bgn</td>
<td>normal</td>
<td>6</td>
<td>15</td>
</tr>
<tr>
<td>ap650-316428</td>
<td>00-23-68-40-68-F0</td>
<td>11an</td>
<td>normal</td>
<td>157+</td>
<td>15</td>
</tr>
<tr>
<td>ap650-316428</td>
<td>00-23-68-40-6C-30</td>
<td>11bgn</td>
<td>normal</td>
<td>1</td>
<td>15</td>
</tr>
<tr>
<td>ap650-860F18</td>
<td>00-23-68-74-C9-20</td>
<td>11an</td>
<td>normal</td>
<td>153+</td>
<td>15</td>
</tr>
<tr>
<td>ap650-860F18</td>
<td>00-23-68-74-CC-50</td>
<td>11bgn</td>
<td>normal</td>
<td>11</td>
<td>15</td>
</tr>
</tbody>
</table>

Total number of radios displayed: 6

### 3.4.2 show smart-rf channel-distribution

To see the channel distribution on the AP radios in the campus, use the command `show smart-rf channel-distribution`

rfs6000-1# show smart-rf channel-distribution

2.4GHz channel distribution for 3 radios

<table>
<thead>
<tr>
<th>CHANNEL</th>
<th>NUM RADIOS</th>
<th>DISTRIBUTION (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>33.33</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>33.33</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>33.33</td>
</tr>
</tbody>
</table>

5GHz channel distribution for 3 radios

<table>
<thead>
<tr>
<th>CHANNEL</th>
<th>NUM RADIOS</th>
<th>DISTRIBUTION (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>149+</td>
<td>1</td>
<td>33.33</td>
</tr>
<tr>
<td>153+</td>
<td>1</td>
<td>33.33</td>
</tr>
</tbody>
</table>
3.4.3 show smart-rf history

To see the actions taken by the Smart-RF, use the command *show smart-rf history*

```
rfs6000-1#show smart-rf history
```

<table>
<thead>
<tr>
<th>TIME</th>
<th>EVENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-06-02 16:49:44</td>
<td>Radio Added</td>
<td>Radio ap650-860F18:R2 (00-23-68-74-C9-20) added</td>
</tr>
<tr>
<td>2012-06-02 16:49:44</td>
<td>Radio Added</td>
<td>Radio ap650-860F18:R1 (00-23-68-74-CC-50) added</td>
</tr>
<tr>
<td>2012-06-02 16:49:44</td>
<td>AP Connected</td>
<td>AP ap650-860F18 master connectivity established</td>
</tr>
<tr>
<td>2012-06-02 15:28:24</td>
<td>Interference Recovery</td>
<td>Radio ap650-316428:R2 (00-23-68-40-68-F0) channel changed from 36 to 157+</td>
</tr>
<tr>
<td>2012-06-02 15:25:41</td>
<td>Interference Recovery</td>
<td>Radio ap650-316428:R1 (00-23-68-40-6C-30) channel changed from 6 to 1</td>
</tr>
<tr>
<td>2012-06-07 18:54:52</td>
<td>Coverage Recovery Done</td>
<td>Radio ap650-316428:R2 (00-23-68-40-68-F0) power changed from 19 to 15</td>
</tr>
<tr>
<td>2012-06-07 18:54:42</td>
<td>Coverage Hole Recovery</td>
<td>Radio ap650-316428:R2 (00-23-68-40-68-F0) power changed from 15 to 19. Coverage hole triggered due to wireless client 00-27-10-29-D2-S8</td>
</tr>
</tbody>
</table>

4. Appendix

4.1 Scaling

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

4.1.1 Access Points

There are various considerations while deciding the number of access points that can be managed by a controller.

4.1.1.1 Wireless controller adoption capacity:

Each Wireless Controller is designed to support a specific number of Access Points, as described in the table below. 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.

<table>
<thead>
<tr>
<th>Wireless Controller Model</th>
<th>Maximum Number of APs</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFS4000</td>
<td>36</td>
</tr>
<tr>
<td>RFS6000</td>
<td>256</td>
</tr>
<tr>
<td>RFS 7000</td>
<td>1024</td>
</tr>
<tr>
<td>NX9500</td>
<td>10,240</td>
</tr>
</tbody>
</table>

Table 4.1.1.1 – Wireless Controller Adoption Capacity

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 adoption capacity for each Wireless Controller. For example assume you have two RFS6000 wireless controllers in a cluster in active-active mode, with 150 access points adopted to each. If one of the wireless controller fails, you will exceed the number of supported access points (256) on a single RFS6000 Wireless Controller. An RFS7000 Wireless Controller for this deployment would be a better choice.

4.1.1.2 Forwarding modes:

When using the local bridging modes, the access points can forward user traffic directly towards it’s destination, and does not need to be tunneled through the controller. In this mode, only the control traffic of around 2-3 kbps per Access point is tunneled through the controller. And we can use the full adoption capacity as mentioned above.

But when the tunnel mode forwarding is used, the traffic is routed through controller, and the controller switching capacity needs to be considered. The amount of user traffic per access point should be estimated to determine the maximum number of access points that can be accommodated. Assuming a user traffic of 20 Mbps (bi-directional) per access point, an RFS7000 can support 200 (4Gbps / 20Mbps) access points. The switching capacity for each controller model is provided below:
<table>
<thead>
<tr>
<th>Wireless Controller Model</th>
<th>Switching Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFS4000</td>
<td>2 GBps</td>
</tr>
<tr>
<td>RFS6000</td>
<td>2 Gbps</td>
</tr>
<tr>
<td>RFS 7000</td>
<td>4 Gbps</td>
</tr>
<tr>
<td>NX9500</td>
<td>NA</td>
</tr>
</tbody>
</table>

*Table 4.1.2 – Wireless Controller Switching capacity*

NX9500 does not support data plane and only supports control plane.

### 4.1.1.3 Number of access points when using tunnel forwarding mode

The tunnel forwarding mode will use MINT to extend the VLANs. It is recommended to restrict the number of access points when using tunnel mode to restrict the control traffic being sent between the access points. The number of access points across when using tunnel mode is given in the table below:

<table>
<thead>
<tr>
<th>Wireless Controller Model</th>
<th>Max Access Point using tunnel mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFS4000</td>
<td>36</td>
</tr>
<tr>
<td>RFS6000</td>
<td>128</td>
</tr>
<tr>
<td>RFS 7000</td>
<td>256</td>
</tr>
<tr>
<td>NX9500</td>
<td>NA</td>
</tr>
</tbody>
</table>

*Table 4.1.3 – Access points using extended VLAN / Wireless Controller*

NX9500 does not support data plane and only supports control plane.
If you want to use tunnel mode beyond this limit, you can consider using L2TPv3 tunneling of the VLAN traffic.

### 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:

Please note that the limits below apply to the controllers when tunneling the user traffic to the controller. When using local bridging mode, these limits are no longer relevant and depend on the number of users each access point can adopt.

<table>
<thead>
<tr>
<th>Wireless Controller Model</th>
<th>Maximum Wireless Users / Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFS4000</td>
<td>500</td>
</tr>
<tr>
<td>RFS6000</td>
<td>2000</td>
</tr>
<tr>
<td>RFS 7000</td>
<td>8000</td>
</tr>
<tr>
<td>NX9500</td>
<td>32,968</td>
</tr>
</tbody>
</table>

*Table 4.1.2.1 – Wireless Users / Controller*

*Table 4.1.2.2 – Wireless Users / Access Point Radio*

<table>
<thead>
<tr>
<th>AP Model</th>
<th>Maximum Wireless Users / AP radio</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP7131</td>
<td>256</td>
</tr>
<tr>
<td>AP7161</td>
<td>256</td>
</tr>
<tr>
<td>AP7181</td>
<td>256</td>
</tr>
<tr>
<td>AP6532/AP650</td>
<td>256</td>
</tr>
<tr>
<td>AP6522/AP622</td>
<td>256</td>
</tr>
<tr>
<td>AP6521/AP621</td>
<td>128</td>
</tr>
<tr>
<td>AP6511</td>
<td>128</td>
</tr>
</tbody>
</table>
The wireless client association limits are the same on per AP and per 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:

<table>
<thead>
<tr>
<th>Wireless Controller Model</th>
<th>Maximum Wireless LANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFS6000</td>
<td>32</td>
</tr>
<tr>
<td>RFS 7000</td>
<td>256</td>
</tr>
<tr>
<td>NX9500</td>
<td>1024</td>
</tr>
</tbody>
</table>

Table 4.1.3 – Wireless LANs / Wireless Controller

### 4.1.4 DHCP Server support

In WiNG 5.x, a DHCP server policy is created with DHCP pools and applied to a device which could be a controller or an access point. While multiple DHCP server policies can be created on a controller, only one DHCP server policy can be applied to a device at a time.

<table>
<thead>
<tr>
<th>DHCP server support on Wireless Controllers</th>
<th>RFS4000</th>
<th>RFS6000</th>
<th>RFS7000</th>
<th>NX9500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of DHCP server policies</td>
<td>36</td>
<td>48</td>
<td>64</td>
<td>4094</td>
</tr>
<tr>
<td>Number of DHCP IP pools per DHCP server policy</td>
<td>128</td>
<td>128</td>
<td>128</td>
<td>128</td>
</tr>
</tbody>
</table>

Table 4.1.4.1 – DHCP server support on Wireless Controllers

<table>
<thead>
<tr>
<th>DHCP server support on Independent Access points, AP71x1, AP6532, AP6521, AP6511</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of DHCP server policies</td>
</tr>
</tbody>
</table>

DHCP server support on Independent Access points, AP71x1, AP6532, AP6521, AP6511
Number of DHCP IP pools per DHCP server policy | 128

**Table 4.1.4.2 – DHCP server support on Independent Access Points**

The DHCP server is not supported on dependent access points, AP650, AP621

### 4.1.5 Firewall ACL rules

The following table indicates the number of firewall IP and MAC rules supported on each platform.

<table>
<thead>
<tr>
<th>Wireless Controller model</th>
<th>Maximum IP ACLs</th>
<th>Maximum MAC ACLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFS4000</td>
<td>512</td>
<td>128</td>
</tr>
<tr>
<td>RFS6000</td>
<td>512</td>
<td>128</td>
</tr>
<tr>
<td>RFS7000</td>
<td>512</td>
<td>128</td>
</tr>
<tr>
<td>NX 9500</td>
<td>4096</td>
<td>256</td>
</tr>
</tbody>
</table>

**Table 4.1.5.1 – Firewall ACL rules / Wireless Controller**

### 4.1.6 Firewall flows

The following table indicates the number of firewall IP and MAC rules supported on each wireless controller platform:

<table>
<thead>
<tr>
<th>Wireless Controller Model</th>
<th>Maximum Firewall Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFS4000</td>
<td>50,000</td>
</tr>
<tr>
<td>RFS 6000</td>
<td>100,000</td>
</tr>
<tr>
<td>RFS7000</td>
<td>200,000</td>
</tr>
</tbody>
</table>
Table 4.1.6.1 – Firewall flows / Wireless Controller

The following table indicates the number of firewall IP and MAC rules supported on each access point platform:

<table>
<thead>
<tr>
<th>Access Point Model</th>
<th>Maximum Firewall Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP71x1</td>
<td>25,804</td>
</tr>
<tr>
<td>AP6532</td>
<td>25,804</td>
</tr>
<tr>
<td>AP6521</td>
<td>6451</td>
</tr>
<tr>
<td>AP6511</td>
<td>6451</td>
</tr>
<tr>
<td>AP650</td>
<td>25,804</td>
</tr>
<tr>
<td>AP621</td>
<td>25,804</td>
</tr>
</tbody>
</table>

Table 4.1.6.2 – Firewall flows / Access Point

4.1.7 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:

<table>
<thead>
<tr>
<th>Wireless Controller Model</th>
<th>Maximum Aggregate profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFS4000</td>
<td>256</td>
</tr>
<tr>
<td>RFS 6000</td>
<td>256</td>
</tr>
<tr>
<td>RFS7000</td>
<td>256</td>
</tr>
<tr>
<td>NX9500</td>
<td>256</td>
</tr>
</tbody>
</table>

Table 4.1.8.1 – Device Profiles / Wireless Controller
4.1.8  MAC address table size

The following table provides the maximum number of MAC Table Entries supported on each hardware platform in WiNG 5.X:

<table>
<thead>
<tr>
<th>Wireless Controller Model</th>
<th>Maximum MAC Table size</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFS4000</td>
<td>64K</td>
</tr>
<tr>
<td>RFS 6000</td>
<td>64K</td>
</tr>
<tr>
<td>RFS7000</td>
<td>64K</td>
</tr>
<tr>
<td>NX9500</td>
<td>64K</td>
</tr>
</tbody>
</table>

Table 4.1.8.1 – MAC Table size / Wireless Controller

<table>
<thead>
<tr>
<th>Access Point Model</th>
<th>Maximum Aggregate profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP7181/AP7161/AP7131</td>
<td>64K</td>
</tr>
<tr>
<td>AP6532/AP650</td>
<td>64K</td>
</tr>
<tr>
<td>AP6522/AP622</td>
<td>64K</td>
</tr>
<tr>
<td>AP6521/AP621</td>
<td>16K</td>
</tr>
<tr>
<td>AP6511</td>
<td>16K</td>
</tr>
</tbody>
</table>

Table 4.1.7.1 – MAC Table size / Access Point

4.2  VLAN planning

The VLANs need to be planned for mapping the wireless users and also to connect the Access points to the Controllers. The application servers, authentication server, DNS, etc have no restriction as long as they have L3 connectivity to the users or the Wireless infrastructure as appropriate. The DHCP server should reside in the same VLAN mapped to the users, or DHCP relay functionality can be used and the DHCP server should have L3 connectivity to the AP or the Wireless Controller.
4.2.1 Access Point VLAN:

The Access point should have at least one management VLAN to communicate with the wireless controller. The access points can be adopted at Layer-2 if they share this VLAN with the wireless controller. If the wireless controller is not present on the same VLAN, then the access points will adopt over Layer-3 to the controllers. The controller ip address could be configured statically, or assigned through DHCP option 191 for plug and play deployment. And it is recommended to have the management VLAN as untagged. If multiple VLANs are mapped to the Ethernet interface of Access points to bridge the wireless client traffic locally, 802.1q VLAN trunking can be used.

4.2.2 User VLAN

There could be various considerations to select the VLAN to be assigned to the wireless users. They could be assigned to a specific VLAN, based on the access restrictions that need to be applied to the user traffic on the wired network. User VLAN pooling can be used to load balance the users across multiple VLANs. The user VLAN can also be assigned to the users by the AAA server, based on the user identity. The user is assigned the same VLAN irrespective of the location it is accessing the wireless network.

The user VLAN can be bridged locally or tunneled to the wireless controller in the data center as described in section 4.1.1.2.

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 Access Points and Wireless Controllers, 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:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>20-21</td>
<td>FTP File Transfer</td>
</tr>
<tr>
<td>TCP</td>
<td>22</td>
<td>SSHv2</td>
</tr>
<tr>
<td>TCP</td>
<td>23</td>
<td>TelNet</td>
</tr>
<tr>
<td>TCP</td>
<td>49</td>
<td>TACACS+ Authentication</td>
</tr>
<tr>
<td>UDP</td>
<td>53</td>
<td>DNS Name Resolution</td>
</tr>
<tr>
<td>Protocol</td>
<td>Port</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>UDP</td>
<td>69</td>
<td>TFTP</td>
</tr>
<tr>
<td>TCP</td>
<td>80</td>
<td>HTTP</td>
</tr>
<tr>
<td>UDP</td>
<td>123</td>
<td>NTP Time Synchronization</td>
</tr>
<tr>
<td>UDP</td>
<td>161</td>
<td>DNMP Device management</td>
</tr>
<tr>
<td>UDP</td>
<td>162</td>
<td>SNMP Traps</td>
</tr>
<tr>
<td>TCP</td>
<td>389</td>
<td>LDAP/Active Directory Authentication</td>
</tr>
<tr>
<td>TCP</td>
<td>443</td>
<td>HTTPS Device Management/ Sensor ➔ ADSP Communication</td>
</tr>
<tr>
<td>TCP</td>
<td>444</td>
<td>HTTPS Captive portal authentication</td>
</tr>
<tr>
<td>TCP</td>
<td>880</td>
<td>HTTP Captive portal authentication</td>
</tr>
<tr>
<td>UDP</td>
<td>1812</td>
<td>Radius Authentication</td>
</tr>
<tr>
<td>UDP</td>
<td>1813</td>
<td>Radius Accounting</td>
</tr>
<tr>
<td>TCP</td>
<td>8443</td>
<td>Sensor ➔ Controller communication (Advanced WIPS)</td>
</tr>
<tr>
<td>UDP</td>
<td>24576</td>
<td>Access Point Adopt</td>
</tr>
</tbody>
</table>

Table 4.3 – WiNG 5.X Protocols & Ports