If you have a WLC in your network plan, you can configure WLC System features using RingMaster.

The following features can be configured:

- Configuring Ports on a WLC
- Overview of Wired Authentication on a WLC
- Configuring Wired Authentication on a WLC
- Creating Port Groups on a WLC
- Creating a Syslog Server
- Configuring Static Routes
- Creating an IP Alias
- Creating an DNS Server
- Creating a NTP Server
- Creating an ARP Entry
- Creating a VLAN Profile
- Configuring Spanning Tree Properties
- Creating an Access Control List (ACL)
- Creating a Quality of Service (QoS) Profile
Configuring Ports on a WLC

You can configure and display information for the following port parameters:

- Name
- State
- Type (network, AP, or wired authentication)
- Speed and autonegotiation
- Power over Ethernet (PoE) state
- Media type (gigabit Ethernet ports only)
- Load sharing (see Port Groups.)

1. From the Organizer panel, select a WLC and then under System, select Ports.
2. To view the 10/100 Ethernet Port Properties, select a Port and then click Properties.
3. The 10/100 Ethernet Port Properties window is displayed.
4. In the Name field, type a port name (1 to 16 alphanumeric characters, no spaces or tabs).
5. The port is enabled by default. To disable the port, clear the Enabled checkbox.
6. Select SNMP Link Traps if desired. By default, notifications for link state changes are disabled. If you enable them, SNMP link traps are sent when the port state changes, and RingMaster also polls and monitors the status of the port. To generate the LinkDown and LinkUp SNMP traps, you must enable this option.
   
   NOTE: You must globally enable SNMP traps in order to receive notification.
7. To specify the speed of a 10/100 Ethernet port, select one of the following:
   - Auto — Sets the port to automatically detect the traffic speed and set the speed accordingly. This is the default value.
   - 10 — Sets the speed to 10 Mbps.
   - 100 — Sets the speed to 100 Mbps.
   
   The port speed for gigabit Ethernet ports is 1000 Mbps and cannot be configured.
8. To specify the operating mode of a 10/100 Ethernet port, select Half for half-duplex or Full for full-duplex mode.
9. To enable PoE on a 10/100 Ethernet port, select PoE Enabled. By default, PoE is disabled. To disable PoE, clear PoE Enabled.
10. For a gigabit Ethernet port (if supported by the WLC), select the interface you want to enable.
   - GBIC — Enables the fiber interface and disables the copper interface.
   - RJ45 — Enables the copper interface and disables the fiber interface.
   
   A port supports only the physical interface you select. The other interface is disabled. The port cannot dynamically move between one interface and the other.
11. To configure Link Layer Discovery Protocol (LLDP) for the selected port, you can select from one of the following Operation Modes:
• **TxRx** — Transmit and Receive LLDP packets.
• **Tx** — Transmit LLDP packets
• **Rx** — Receive LLDP packets
• **None** — Disable LLDP on the port.

12. Click **Save**.
Changing Port Settings on a WLC

Gigabit Ethernet Port Properties

1. In the Organizer panel, select a WLC from the list.
2. Expand the System options, and select Ports.
3. Select a port from the Gigabit Ethernet Port list and click Properties.
4. In the Name field, type a port name (1 to 16 alphanumeric characters, no spaces or tabs).
5. Clear the Enabled checkbox if you want to disable the port. Click OK to complete the configuration. If you want to make additional changes to the settings, go to the next step.
6. Select SNMP Link Traps if desired. By default, notifications for link state changes are disabled. If you enable them, SNMP link traps are sent when the port state changes, and RingMaster also polls and monitors the status of the port. To generate the LinkDown and LinkUp SNMP traps, you must enable this option.
7. The port speed for gigabit Ethernet ports is 1000 Mbps and cannot be configured.
8. The operating mode for a gigabit port is Full duplex by default.
9. Auto-negotiation is enabled by default.
10. PHY Media Type is SMF by default.
11. From the PHY Media Preference list, select RJ45 or SFP.
12. Click OK to save the configuration.

10 Gigabit Ethernet Port

1. In the Organizer panel, select a WLC from the list.
2. Expand the System options, and select Ports.
3. Select a port from the 10 Gigabit Ethernet Port list and click Properties.
4. In the Name field, type a port name (1 to 16 alphanumeric characters, no spaces or tabs).
5. Clear the Enabled checkbox if you want to disable the port. Click OK to complete the configuration. If you want to make additional changes to the settings, go to the next step.
6. Select SNMP Link Traps if desired. By default, notifications for link state changes are disabled. If you enable them, SNMP link traps are sent when the port state changes, and RingMaster also polls and monitors the status of the port. To generate the LinkDown and LinkUp SNMP traps, you must enable this option.
7. The port speed for 10 Gigabit Ethernet ports is 10Gbps and cannot be configured.
8. The operating mode for a gigabit port is Full duplex by default.
9. Auto-negotiation is enabled by default.
10. PHY Media Type is XFP by default.
11. the PHY Media Preference is None by default.
12. Click OK to save the configuration.
Overview of Wired Authentication on a WLC

A wired authentication port is an Ethernet port that has 802.1X authentication enabled for access control. Like wireless users, users that are connected to the WLC over Ethernet can be authenticated before they can be authorized to use the network. However, data for wired users is not encrypted after they are authenticated.

Informational Note:
For 802.1X clients, wired authentication works only if clients are directly attached to a wired authentication port, or attached through a hub that does not block forwarding of packets from a client to the PAE group address (01:80:c2:00:00:03). Wired authentication works in accordance with 802.1X specification, which prohibits a client from sending traffic directly to the MAC address of an authenticator until the client is authenticated.

Instead of sending traffic to the MAC address of an authenticator, a client sends packets to the PAE group address. The 802.1X specification prohibits networking devices from forwarding PAE group addresses packets, because this would make it possible for multiple authenticators to acquire the same client. For non-802.1X clients who use MAC authentication, WebAAA, or last-resort authentication, wired authentication works whether clients are directly attached or indirectly attached.

Informational Note:
If you plan to specify a RADIUS server group, configure the group first, before using the wizard. The wizard does not provide a way to configure RADIUS servers or groups. (See RADIUS.)

To configure Wired Auth, see “Configuring Wired Authentication on a WLC”.
Configuring Wired Authentication on a WLC

1. In the Tasks panel under Setup, click Wired Auth.
2. The Configure Wired Auth wizard is displayed.

Selecting Open Access for Wired Authentication

3. Select Open Access from the Fall Through Authentication list to automatically authenticate the client and allow access to the SSID requested by the client, without requiring a username and password from the client.

Selecting Web Portal for Wired Authentication

4. From the Fall Through Authentication list, select Web Portal to serve the client a web page from the nonvolatile storage of the WLC for login to the SSID.

Selecting None for Wired Authentication

5. From the Fall Through Authentication list, select None to deny authentication and prohibit the client from accessing the SSID. This is the default.

6. To configure the maximum number of sessions, enter the number or use the up and down arrows. By default, only 1 session is allowed.

7. Enable Idle Timeout is selected by default. To disable this option, clear the checkbox.

8. Configure the maximum number of seconds that a client can be idle before the session is timed out. The default value is 300 seconds (five minutes).

9. Click Next.

10. From the VLAN Name list, select the VLAN used by wireless clients. Click Next.

Create AAA Access

11. To allow 802.1X access, you must configure access rules that specify the AAA servers to use for authentication. If you have not previously configured a rule, click Create.

12. Enter a userglob to match specific usernames. or "**" as a wildcard to match all users. ** is the default value.

13. From the EAP Type list, select from the following options:
   - External Authentication Server
   - EAP-MD5 Offload
   - PEAP Offload - if you select PEAP Offload, then MS-CHAPV2 is selected as the EAP Sub-protocol by default.
   - Local EAP-TLS

14. Click Next.

15. Add Authentication Servers from the Available AAA Server groups to the Current AAA Server Groups. Select LOCAL to use the database on the WLC.

Create 802.1X Rules
   See Configuring 802.1X Global Parameters.

MAC Access Rules
   See Creating a MAC Access Rule.

Local User Database
   See Creating Users in the Local User Database.
   17. Click **Finish** to complete the configuration.
Creating Port Groups on a WLC

A port group is a set of physical ports that function together as a single link and provide load sharing and link redundancy. Only network ports can participate in a port group. The WLC assigns traffic flows to ports based on the source and destination MAC addresses of the traffic, which balances port group traffic among the physical ports of the group. The WLC assigns a traffic flow to an individual port in the group and uses the same port for all subsequent traffic for that flow.

A port group ensures link stability by providing redundant connections for the same link. If an individual port in a group fails, the WLC reassigns traffic to the remaining ports. When the failed port starts operating again, the WLC begins using it for new traffic flows. Traffic that belonged to the port before it failed continues to be assigned to other ports.

Layer 2 configuration changes apply collectively to a port group as a whole but not to individual ports within the group. For example, Spanning Tree Protocol (STP) changes affect the entire port group rather than individual ports. When you make Layer 2 configuration changes, you can use a port group name in place of the port list. Ethernet port statistics continue to apply to individual ports and not to port groups.

Configuring Port Groups

1. In the Tasks panel, select Create Port Group. The Create Port Group wizard is displayed.
2. In the Port Group Name field, type the name of the port group (1 to 16 alphanumeric characters, with no spaces or tabs). Click Next.
3. The Port Group Members list is displayed.
4. To add a port to a port group, select it from the Member list. To remove a Member, clear the Member checkbox.
5. To change the membership of a port in another port group, select Member for the port. The Port Group Member Remove dialog appears. Click Yes to change membership. Click No to leave the membership unchanged.
6. Click Finish.
Configuring Management Services on a WLC

1. From the Organizer panel, select a WLC.
2. Select System, and then Management Services.
3. You can manually select a service from the list of Management Services. You can select any of the following options:
   - HTTPS
   - Telnet
   - SSH
   - Web Portal
   - SNMP
   - TFTP
4. To change the idle timeout for CLI sessions, edit the value in the Idle Timeout field. You can specify from 0 to 86400 seconds (one day). The default is 3600 (one hour). If you specify 0, the idle timeout is disabled. The timeout interval is in 30-second increments. For example, the interval can be 0, or 3 seconds, or 60 seconds, or 90 seconds, and so on. If you enter an interval that is not divisible by 30, the WLC rounds up to the next 30-second increment.
5. Select the port number for Management Port. The default value is 3002.
6. Select the port number for HTTP Port. The default value is 80.
7. Select the port number for HTTPS Port. The default value is 23.
8. Select the port number for Telnet. The default value is 23.
9. Select the port number for SSH. The default value is 22.
10. Select the SSL Mode from the list. You can configure Partial, All, or None.
11. Specify the port number for TFTP Services.
Configuring SNMP Using SNMP V1 or V2c

On each WLC in the network plan, you must enable notifications and configure RingMaster Services as a notification target (trap receiver). RingMaster Services software does not start listening for SNMP notifications from an WLC until you add RingMaster Services as an SNMP notification target to the WLC. (For simple configuration of RingMaster Services as an SNMP notification target, see System Setup Wizard.)

To configure SNMP v1 using RingMaster, use the following steps:

1. From the Organizer panel, select a WLC from the list.
2. Expand System and select Management Services.
3. From the list of Management Services, select SNMP.
4. In the SNMP interface, select V1 or V2c.
5. From the Task Panel under Create, select Create Community.
6. The Create Community wizard is displayed.
7. In the Community String field, type the name of the community. The name can be 1 to 32 alphanumeric characters, with no spaces or tabs.
   
   **NOTE:** Community string names are transmitted in clear text.
   
   **NOTE:** If you enable SNMP service on the WLC, Juniper Networks recommends that you do not use the well-known strings public (for READ) or private (for WRITE). These strings are commonly used and can easily be guessed.

8. Select the access type:
   
   - **Read-Only** — An SNMP management application using the string can get (read) object values on the WLC but cannot set (write) them. This is the default.
   
   - **Read-Notify** — An SNMP management application using the string can get object values on the WLC but cannot set them. The WLC can use the string to send notifications.
   
   - **Read-Write-Notify** — An SNMP management application using the string can get and set object values on the WLC.
   
   - **Read-Write** — An SNMP management application using the string can get and set object values on the WLC. The WLC can use the string to send notifications.
   
   - **Notify-Only** — The WLC can use the string to send notifications.

9. Click OK.
Setting Up Trap Logging

1. From the Organizer panel, select a WLC.
2. From System, select Management Services.
3. Under SNMP in the Configuration pane, select Trap Log.
4. From the Tasks panel, under Setup, click Trap Logging.
5. You can log all or some of the following SNMP traps:
   - Authentication
   - LinkDown
   - LinkUp
   - DeviceFail
   - DeviceOkay
   - PoEFail
   - MobilityDomainJoin
   - MobilityDomainTimeout
   - RFDetectAdhocUser
   - ClientAuthenticationFailure
   - ClientAuthorizationFailure
   - ClientAuthorizationSuccess
   - ClientAssociationFailure
   - ClientRoaming
   - ClientDeAssociation
   - AutoTuneRadioChannelChange
   - AutoTuneRadioPowerChange
   - CounterMeasureStop
   - CounterMEasureStart
   - ClientCleared
   - ClientDot1xFailure
   - RFDetectClientViaRogueWiredAP
   - RFDetectDoS
   - ClientAssociationSuccess
   - RFDetectDoSPort
   - RFDetectAdhocUserDisappear
   - ClientIpAddrChange
   - ClientAuthenticationSuccess
   - ClientDeAuthentication
- ClientDeviceProfileChangeTraps
- ClientDeviceTypeChangeTraps
- MobilityDomainFailOver
- MobilityDomainFailBack
- ApRejectLicenseExceeded
- RFDetectBlacklisted
- RFDetectClassificationChange
- ClientDisconnect
- ClientDynAuthorChangeFailure
- ClientDynAuthorChangeSuccess
- RFDetectRogueDevice
- APOperRadioStatus2
- APNonOperStatus2
- ConfigurationSaved
- MichaelMICFailure
- RFDetectSuspectDeviceDisappear
- RFDetectSuspectDevice
- RFDetectRogueDeviceDisappear
- ClusterFail
- MobilityDomainResiliencyStatus
- ApManagerChange
- MultimediaCallFailure
- WLCTunnelLimitExceeded
- RFNoiseSource

6. Click **OK**.
Configuring SNMP Views

1. From the Organizer panel, select a WLC.
2. From System, select Management Services.
3. From the Tasks panel, under Create, click Create View.
4. In the View Name field, type the name of the view. The name can be 1 to 15 alphanumeric characters, with no spaces or tabs.
5. Enter a description of the View.
6. From the Root OID list, select None, Included or Excluded.
7. Define the SNMP Tree by adding in a subtree. This can be a name or an object ID.
8. Select Included or Excluded from the Type list.
9. Click Finish.
10. Click Ok to accept the configuration.
Configuring SNMP Groups

1. From the Organizer panel, select a WLC.
2. From System, select Management Services.
3. From the Tasks panel, under Create, click Create Group.
4. In the Group Name field, type the name of the group. The name can be 1 to 15 alphanumeric characters, with no spaces or tabs.
5. Enter a description of the group.
6. Click Next.
7. Define the access permissions for this group by specifying the read, write, or notify view.
8. To add an Access Entry, click Add Access Entry. You can select one set of values for each security pair:
   a. From the Security Model, select V1, USM, or V2C.
   b. From the Security Level, select No Authen, No Priv. If you select USM, you can select from Auth & Priv, Authen, No Priv, or No Authen, No Priv.
   c. Configure the Read View, Write View or Notify View.
   d. Click OK.
9. Click Finish.
Configuring SNMP Using USM

1. Access the Create USM User wizard:
2. Select the Configuration Navigation Bar button.
3. In the Organizer panel, click the plus sign next to an WLC.
4. Click the plus sign next to System.
5. Select Management Services.
6. In the Tasks panel, select Create USM User.
7. In the Username field, type the name of the SNMPv3 user. The name can be 1 to 32 alphanumeric characters, with no spaces or tabs.
8. Select the access type.
   - Read-Only — An SNMP management application using the string can get (read) object values on the WLC but cannot set (write) them. This is the default.
   - Read-Notify — An SNMP management application using the string can get object values on the WLC but cannot set them. The WLC can use the string to send notifications.
   - Read-Write-Notify — An SNMP management application using the string can get and set object values on the WLC.
   - Read-Write — An SNMP management application using the string can get and set object values on the WLC.
   - Notify-Only — The WLC can use the string to send notifications.
9. Specify the Engine ID, which is the unique identifier for this instance of the SNMP engine:
10. Select the format:
    - Hex — ID is a hexadecimal string.
    - IP — ID is based on the IP address of the station running the management application. Enter the IP address of the station. MSS calculates the engine ID based on the address.
    - LocalID — Uses the value computed from the system IP address for the WLC.
11. NOTE: To send informs, you must specify the engine ID of the inform receiver. To send traps and to allow get and set operations and so on, specify local as the engine ID.
12. If you select Hex or IP, type the hexadecimal string or IP address in the Value field and click Next and go to Step 5. Otherwise, click Finish.
13. Select the authentication type used to authenticate communications with the remote SNMP engine:
    - None — No authentication is used. This is the default.
    - MD5 — Message-digest algorithm 5 is used.
    - SHA — Secure Hashing Algorithm (SHA) is used.
14. If you select MD5 or SHA, you can specify a passphrase or hexadecimal key:
    - Select the format from the Format list.
    - Type the value in the Password field.
• If you selected Key as the format, type a 16-byte hexadecimal string for MD5 or a 20-byte hexadecimal string for SHA.

• If you selected Pass Phrase as the format, type a string at least 8 characters long.

15. Select the encryption type used for SNMP traffic:
   • None — No encryption is used. This is the default.
   • DES — Data Encryption Standard (DES) encryption is used.
   • 3DES — Triple DES encryption is used.
   • AES — Advanced Encryption Standard (AES) encryption is used.

16. If you select DES, 3DES, or AES, you can specify a passphrase or a hexadecimal key:
   • Select the format from the Format pull-down list.
   • Type the value in the Password field.
   • If you selected Key as the format, type a 16-byte hexadecimal string.
   • If you selected PassPhrase as the format, type a string at least 8 characters long for DES or 3DES, or at least 12 characters long for AES.
   • Click Finish.
Configuring a Notification Profile for SNMP

A notification profile is a named list of all of the notification types that can be generated by a WLC, and for each notification type, the action to take (drop or send) when an event occurs.

1. Access the Create Notification Profile wizard.
2. Select the Configuration Navigation Bar button.
3. In the Organizer panel, click the plus sign next to an WLC.
4. Click the plus sign next to System.
5. Select Management Services.
6. In the Tasks panel, select Create Notification Profile.
7. In the Profile Name field, type the notification profile name. It can be 1 to 32 alphanumeric characters, with no spaces or tabs. The Notification Profile Traps dialog appears.
8. Click the checkbox next to each notification type you want to enable. To enable all notification types, select Enable at the top of the list.
9. Click Finish.

Setting Up a Notification Target for SNMP

You can configure a different IP address to use the source IP address for SNMP traps. To do this, you can configure notification targets for SNMP using these steps:

1. Select the Configuration Navigation Bar button.
2. In the Organizer panel, click the plus sign next to an WLC.
3. Click the plus sign next to System.
4. Select Management Services.
5. Click Setup Notification Target to display the wizard.
6. The ID, IP Address, and Port are set by default. The IP address is the IP address of the RingMaster server.
7. To use a different IP address as the source IP address, enter the desired IP address in the Source IP field.
8. Click Next.
9. Select the desired traps to send as SNMP traps.
10. Enter a name in the Community String field.
11. Select Access or Group.
12. Select from Notify-Only, Read-Notify, or Read-Write-Notify.
13. Click Finish to save the configuration.
To modify a Notification Target, select it from the list, and click Properties.
Configuring SNMP Communities

1. From the Organizer panel, select a WLC.
2. From System, select Management Services.
3. From the Tasks panel, under Create, click Create Community.
4. In the Community String field, type the name of the community. The name can be 1 to 32 alphanumeric characters, with no spaces or tabs.
   These strings are transmitted in clear text, and it is recommended that you do not use the string public (for READ) or private (for WRITE). These strings are commonly used and can be easily guessed.
5. Select Access or Group.
6. Configure access by selecting from the Access type list.
   - Read-Only — An SNMP management application using the string can get (read) object values on the WLC but cannot set (write) them. This is the default.
   - Read-Notify — An SNMP management application using the string can get object values on the WLC but cannot set them. The WLC can use the string to send notifications.
   - Read-Write-Notify — An SNMP management application using the string can get and set object values on the WLC.
   - Read-Write — An SNMP management application using the string can get and set object values on the WLC. The WLC can use the string to send notifications.
   - Notify-Only — The WLC can use the string to send notifications.
7. Click OK.
Enabling Syslog Features

Log and Trace Settings

System logs provide information about system events that you can use to monitor and troubleshoot MSS. Event messages for the WLC and the associated WLAs can be stored or sent to the following destinations:

- Stored in a local buffer on the MX
- Displayed on the MX console port
- Displayed in an active Telnet session
- Sent to one or more syslog servers, as specified in RFC 3164

The system log is a file in which the newest record replaces the oldest. These entries are preserved in nonvolatile memory through system reboots.

Traces enable you to perform diagnostic routines. You can set a trace with a keyword, such as authentication or sm, to trace activity for a particular feature, such as authentication or the session manager.

Enabling Syslog Features

1. From the Organizer panel, select a WLC.
4. To enable console logging, select Console Enabled.
5. To enable session logging, select Session Enabled.
6. To enable trace logging, select Trace Enabled.
7. From the Severity Filter list, select from the following:
   - Emergency
   - Alert
   - Critical
   - Error (Default)
   - Warning
   - Notice
   - Info
   - Debug (All)
8. From the Console Severity Filter list, select from the following:
   - Emergency
   - Alert
   - Critical
   - Error (Default)
   - Warning
9. From the **Session Filter Severity** list, select from the following:
   - Emergency
   - Alert
   - Critical
   - Error
   - Warning
   - Notice
   - Info (Default)
   - Debug (All)

10. From the **Trace Severity Filter** list, select from the following:
   - Emergency
   - Alert
   - Critical
   - Error
   - Warning
   - Notice
   - Info
   - Debug (All)

11. Click **Save** to save the configuration.

12. To deploy the changes on the network, click **Deploy**.
Creating an External Syslog Server

1. From the Organizer panel, select a WLC.
3. From the Tasks panel, select Create Syslog Server.
4. Under Syslog Server, enter the IP Address of the Syslog Server.
5. You can change the port or leave it at the default value of 514.
6. You can select from the following Severity Filters:
   - Emergency — The WLC is down.
   - Alert — Action must be taken immediately.
   - Critical — You must resolve the critical situation. If left unresolved, the WLC can reboot or shutdown.
   - Error — WLC is missing data or unable to form a connection.
   - Warning — A possible problem exists.
   - Notice — Events that can cause system problems have occurred. These are logged for diagnostic purposes.
   - Info — Informational messages only No problems exist.
   - Debug (All) — Output from debugging.
   The default severity level is Error.
7. To map all of the facilities to a standard local facility, select Facility Mapping. Some syslog servers require the facility to be set to a standard local facility name.
8. From the Map to Local Facility list, select from Local 0 to Local 7.
9. Click Finish to save the configuration.
Creating a Trace Area

1. From the Organizer panel, select a WLC.
3. From the Tasks panel, select Create Trace Area.
4. Under Trace Area, select the area to trace for logging purposes.
5. Select the trace level from the Level list. The default value is 5 and has a range of 0 to 10.0 provides the minimum amount of information and 10 proves the maximum amount of information.

Optional Parameters
6. In the User Name field, enter the user name to trace on the network. Specify a username no longer than 60 alphanumeric characters with no spaces or tab characters.
7. In the MAC Address field, type the MAC address to trace on the network. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
8. In the Port Name field, type the name of the port to trace on the network.
9. Click Finish to complete the configuration.
Configuring Static Routes

The IP routing table contains routes that MSS uses for determining the external communication interfaces for a WLC. When you add an IP interface to an active VLAN, MSS automatically adds corresponding entries to the IP routing table. For destination routes that are not directly attached, you can add static routes. A static route specifies the destination and the default router through which to forward traffic. You can add the following types of static routes:

- **Explicit route** — Forwarding path for traffic to a specific destination.
- **Default route** — Forwarding path for traffic to a destination without an explicit route.

If the IP routing table contains an explicit route for a given destination, MSS uses the route. Otherwise, MSS uses a default route. (For more information about static routes, see the “Configuring and Managing IP Routes” section in the “Configuring and Managing IP Interfaces and Services” chapter of the Juniper Networks Mobility System Software Configuration Guide.)

Configure a static route if a gateway is configured on the network.

1. Select an existing route or click Create.

2. If you select an existing route, you can highlight it in the list and click Properties to display information about the route. If you click Create, then you can configure a new route on the network.
   a. When you click Create, the Create Route interface is displayed. You can select Default Route to configure the network traffic to use this IP address for routing traffic.
   b. Enter a destination IP address, the Gateway IP address, and the metric for the route. Click OK to save the route configuration.

3. Click Next.
Creating an IP Alias

You can map an IP address to a name by creating an IP alias. For example, if you create an IP alias carmel for IP address 10.20.30.40, you could type telnet carmel rather than telnet 10.20.30.40. You can use IP aliases in conjunction with DNS. If you use IP aliases and DNS is enabled, the WLC looks up IP aliases before checking for entries on a DNS server.

1. From the Organizer panel, select a WLC.
2. From the Task panel, under Create, click Create IP Alias.
3. Enter a Host Name and a Host IP Address.

Informational Note:
You cannot use the word all in the host name.

4. Click OK to save the configuration.
Creating an DNS Server

You can configure an WLC to resolve hostnames to IP addresses by querying a Domain Name Service (DNS) server. By enabling DNS, you can specify a hostname rather than an IP address. For example, rather than typing telnet 10.1.2.3, you could type telnet monterey.example.com. By default, DNS is not enabled. You can specify one primary DNS server and up to five secondary DNS servers.

You configure DNS by performing the following tasks:

- Enable the DNS client and configure a default domain name for DNS queries.
- Specify the IP addresses of the DNS servers.
  1. From the Organizer panel, select a WLC.
  2. From the Task panel, under Create, click Create DNS Server.
  3. Enter the server IP Address and select Primary or Secondary from the Preference list. You can designate only one DNS server as the primary DNS server. All other DNS servers are secondary servers.
  4. Select Enabled under DNS Service.
  5. Enter the Default DNS Domain.
  6. Click OK to save the configuration.
Creating a NTP Server

You can configure an WLC to use the Network Time Protocol (NTP) to automatically set the system date and time. NTP polls network time servers at regular intervals and synchronizes the system date and time with the servers. By default, NTP is not enabled. You can specify up to three NTP servers.

**Informational Note:**
If NTP is configured on a system where the current time differs from the NTP server time by more than 10 minutes, convergence of the WLC time can take many NTP update intervals. Juniper Networks recommends that you set the time manually to the NTP server time before enabling NTP to avoid a significant delay in convergence.

1. From the Organizer panel, select a WLC.
2. From the Task panel, under Create, click **Create NTP Server**.
3. Enter the server IP Address and click **OK** to save the configuration.
4. To enable the NTP Service, select **Enabled** under NTP Client.
5. You can customize the Update Interval [seconds] or leave at the default value of 64. The range is 16 to 1024 seconds.
Creating an ARP Entry

The Address Resolution Protocol (ARP) table maps IP addresses to MAC addresses. ARP is enabled by default on the WLC and cannot be disabled. An ARP entry is added to the table in one of the following ways:

- Automatically by an WLC — The WLC adds a local entry for its MAC address and adds dynamic entries for addresses learned from traffic received by the WLC. When an WLC receives an IP packet, it adds the source MAC address and source IP address of a packet to the ARP table.

- By the system administrator — Using RingMaster, you can add permanent entries to the ARP table. Permanent entries do not age out and remain in the table even after the WLC is rebooted.

1. From the Organizer panel, select a WLC.
2. From the Task panel, under Create, click CreateARP Entry.
3. Enter the IP Address and MAC Address.
4. Click OK to save the configuration.

In the optional Aging Time field, specify the amount of time a dynamic entry can remain unused before the entry is removed from the ARP table. The value range for the aging timeout is 0 to 1,000,000 seconds. The default value is 1200 seconds. To disable aging, specify 0 as the aging timeout. The local entry for an WLC, static entries, and permanent entries in the ARP table are not affected by the aging timeout.
Overview of VLANs

A virtual LAN (VLAN) is a Layer 2 broadcast domain that can span multiple wired or wireless LAN segments. Each VLAN is a separate logical network, and, if you configure IP interfaces on the VLANs, MSS treats each VLAN as a separate IP subnet.

Configure VLANs on the network ports of a WLC by configuring them on the WLC. Configure a VLAN by assigning a name and network ports to the VLAN. Optionally, you can assign VLAN tag values on individual network ports. You can configure multiple VLANs on the network port of a WLC. Optionally, each VLAN can have an IP address.

You do not need to configure VLANs on AP access ports or wired authentication ports, because the VLAN membership of these types of ports is determined dynamically through the authentication and authorization process. Users who require authentication connect through WLC ports that are configured for AP access points or wired authentication access. Users are assigned to VLANs automatically through authentication and authorization mechanisms such as 802.1X. By default, none of the ports of a WLC are in VLANs. A WLC cannot forward traffic on the network until you configure VLANs and add network ports to those VLANs.

Users and VLANs

When a user successfully authenticates to the network, the user is assigned to a specific VLAN. A user remains associated with the same VLAN throughout the user’s session on the network, even when roaming from one WLC to another within a Mobility Domain.

You assign a user to a VLAN by setting one of the following attributes on the RADIUS servers or in the local WLC user database:

- **Tunnel-Private-Group-ID** — This attribute is described in RFC 2868, RADIUS Attributes for Tunnel Protocol Support.
- **VLAN-Name** — This attribute is a Trapeze vendor-specific attribute (VSA).

**Informational Note:**

You cannot configure the Tunnel-Private-Group-ID attribute in the local user database.

Specify a VLAN name, not the number. If both attributes are used, the WLC uses the VLAN name in the VLAN-Name attribute.
Roaming and VLANs

WLCs in a Mobility Domain contain a user traffic within the VLAN assigned to the user. For example, if you assign a user to VLAN red, the WLCs in the Mobility Domain contain the user traffic within VLAN red configured on the WLCs. The WLC that authenticates a user must be a member of the Mobility Domain assigned to that user. You are not required to configure a VLAN on all WLCs in a Mobility Domain. When a user roams to a WLC that is not a member of the VLAN the user is assigned to, the WLC can tunnel traffic for that user through another WLC that is a member of the VLAN.

Informational Note:

Because the default VLAN might not be in the same subnet on each WLC, you should not rename the default VLAN or use it for user traffic. Instead, configure other VLANs for user traffic.
Configuring VLANs

1. Configure VLAN information. You can select a VLAN from the list or create a new. Click **Create** to create a new VLAN.

2. Enter a unique name for the VLAN and the VLAN ID. In the **VLAN Name** field, type a name for the VLAN (1 to 16 alphabetic characters long, with no spaces or tabs). You cannot use a number as the first character in a VLAN name. VLAN names must be globally unique across a mobility domain to ensure intended user connectivity as determined through authentication and authorization. Every VLAN on an WLC has a VLAN name for authorization and a VLAN number. VLAN numbers vary for each WLC and are not related to 802.1Q tag values if used.

3. Optionally, you can select ports or port groups to be members of the VLAN. Do one of the following:
   - To add a port or port group to the VLAN and remove previous VLAN membership, click **Move**.
   - Moving a port or port group could potentially affect multiple VLANs.
   - To add a port or group to a VLAN and retain previous VLAN membership, click **Add**.

4. Click **Next**.

5. Optional VLAN Interface: Select an existing route or click **Create**.
   a. Statically configure an address by editing the IP address and subnet mask (for example, 10.10.10.10/16).
   b. Select DHCP Client to use a DHCP server to dynamically obtain an IP address for the VLAN.

Generally, VLANs are equivalent to IP subnets. If an WLC is connected to the network by only one IP subnet, the WLC must have at least one VLAN configured. Optionally, each VLAN can have its own IP address. However, no two IP addresses on the WLC can belong to the same IP subnet.

**Informational Note:**
MSS does not support assigning the system IP address of a WLC to an address received through the DHCP client. you should use the DHCP client only on WLC2 WLCs you plan to configure using the drop-ship method.

6. Click **OK** to save the route configuration.

7. Click **Next**, and click **Finish** to complete the configuration.

**Changing VLAN Membership**
A port or port group can be in one or more VLANs. To be in multiple VLANs, the port or group must have an 802.1Q VLAN tag. A tag is a numeric value that identifies a virtual port within a VLAN. The same VLAN can have different tag values on different ports. However, a port can have only one tag value in a given VLAN. A VLAN can also have untagged ports. An untagged port can be a member of only one VLAN.

MSS supports the IEEE 802.1Q tag type, described in the IEEE 802.1Q specification.
The tagging capabilities of the WLC are flexible. You can assign 802.1Q tag values on a per-VLAN, per-port basis. The same VLAN can have different tag values on different ports. In addition, the same tag value can be used by different VLANs but on different network ports. If you use a tag value, Juniper Networks recommends that you use the same value as the VLAN number. MSS does not require the VLAN number and tag value to be the same, but other vendors may require it.

**Informational Note:**

Do not assign the same VLAN multiple times using different tag values to the same network port. Although MSS does not prohibit you from doing so, this configuration is not supported.
Configuring VLAN Pooling

Overview

VLAN Pooling is a new feature that allows you to associate "equivalent" VLANs to a service which then improves scalability and reduces broadcast domains across VLANs. Multiple VLANs can be grouped to form a VLAN Pool and all VLANs in the VLAN Pool are available at any time in a location. VLAN assignment is performed dynamically when a wireless client accesses the network and a VLAN is assigned to the wireless client.

For example, if an enterprise network has 1000 wireless clients that can connect to the network from any location in the enterprise, five VLANs may be required to support the client load. The 5 VLANs are then placed into a VLAN pool which is available at any time on the enterprise network. When a wireless client accesses the network, the client is assigned a VLAN, typically one with the fewest clients based on the current client counts on the VLANs in the VLAN Pool by using a round robin algorithm.

The VLAN pool can also be configured on an AAA server.

VLAN Pools can be applied to the following attributes:

- Users
- User Groups
- MAC Users
- MAC User Groups
- Service Profiles

Configuring VLAN Pools

To configure VLAN Pools, select VLAN Pools located in the Organizer.

Once you select VLAN Pools, click Create VLAN Pools from the Task list. A configuration wizard allows you to add VLANs to VLAN Pools.
Configuring Spanning Tree Properties

The standard STP timers delay traffic forwarding briefly after a topology change. The time a port takes to change from the listening state to the learning state or from the learning state to the forwarding state is called the forwarding delay. In some configurations, this delay is unnecessary.

The WLC provides the following fast convergence features to bypass the forwarding delay:

- **Backbone fast convergence** — Backbone fast convergence accelerates the recovery of a port following the failure of an indirect link. Normally, when a forwarding link fails, a bridge that is not directly connected to the link does not detect the link change until the maximum age timer expires. Backbone fast convergence enables the WLC to listen for bridge protocol data units (BPDUs) sent by a designated bridge when the designated link of a bridge to the root bridge fails, and immediately verifies whether BPDU information stored on a port is still valid. If the BPDU information on the port is no longer valid, the bridge immediately starts the listening stage on the port.

  
  **Informational Note:**
  
  If you plan to use the backbone fast convergence feature, enable it on all of the bridges in a spanning tree.

- **Uplink fast convergence** — Uplink fast convergence enables an WLC that has redundant links to the network core to immediately change the state of a backup link to forwarding if the primary link to the root fails. Uplink fast convergence bypasses the listening and learning states to immediately enter the forwarding state.

  
  **Informational Note:**
  
  The uplink fast convergence feature is applicable to bridges that are acting as access WLCs to the network core (distribution layer) but are not in the core themselves. Do not enable the feature on WLCs that are in the network core.

1. From the Organizer panel, select a WLC.
2. Under **System**, select **VLANs**.
3. Under **Spanning Tree Properties**, you can select **Enable Uplink Fast** and **Enable Backbone Fast**.

Changing VLAN Spanning Tree Settings

The purpose of the Spanning Tree Protocol (STP) is to maintain a loop-free network. A loop-free path is accomplished when a device recognizes a loop in the topology and blocks one or more redundant paths. Mobility System Software (MSS) supports 802.1D and Per-VLAN Spanning Tree protocol (PVST+).

- MSS uses 802.1D bridge protocol data units (BPDUs) on VLAN ports that are untagged. However, each VLAN still runs its own instance of STP, even if two or more VLANs contain untagged ports. To run a single instance of STP in 802.1D mode on the entire MX, configure all network ports as untagged members of the same VLAN.
MSS uses PVST+ BPDUs on VLAN ports that are tagged. PVST+ BPDUs include tag information in the 802.1Q field of the BPDUs. MSS runs a separate instance of PVST+ on each tagged VLAN.

**Informational Note:**
When you create a VLAN, STP is disabled on the new VLAN by default, regardless of the STP state of other VLANs on the WLCs.

**Informational Note:**
IEEE 802.1D spanning tree specifications refer to networking devices that forward Layer 2 traffic as bridges. In this context, a WLC is a bridge. Where this manual or the product interface uses the term bridge, you can assume the term is applicable to the WLC.

To change the STP settings of a VLAN:

1. Access the VLAN Properties multi-tabbed dialog box, then click on the **Spanning Tree** tab.

**Informational Note:**
This configures STP features for an individual VLAN but does not configure fast convergence features, which are global.

2. To enable STP, click **Enabled**.

3. Fill in the **Instance Number** field. In the Bridge Priority field, specify the priority of the STP bridge (0 to 65,535). The default is 32,768. The bridge with the lowest priority value becomes the root bridge for the spanning tree.

4. In the **Protocol** field, specify the maximum age value (6 to 40 seconds), which controls how long information from other bridges is kept. The default is 20 seconds.

5. In the **Max Age** field, specify the maximum age value (6 to 40 seconds), which controls how long information from other bridges is kept. The default is 20 seconds.

6. In the **Hello Time** field, specify the interval (1 to 10 seconds) between each configuration message from the root bridge. The default is 2 seconds.

7. In the **Forward Delay** field, specify the amount of time (4 to 30 seconds) a bridge waits after a topology change to begin forwarding data packets. The default is 15 seconds. Click **OK**.

**Changing STP Port Settings in a VLAN**

To change the STP Port settings of a VLAN:

1. Access the VLAN Properties multi-tabbed dialog box, then click on the **Spanning Tree Ports** tab.
2. To enable spanning tree packet processing (Tx/Rx) on that port, make sure Enabled is selected. This is the default. To disable this feature, clear Enabled. If you disable spanning tree packet processing on the port, the following might happen:
   - If STP is enabled on the VLAN, spanning tree packets are dropped at the port.
   - If STP is disabled on the VLAN, spanning tree packets are forwarded transparently through the VLAN to and from that port.

3. In the Port Priority field, specify a priority value (0 to 255). The default is 128.

4. In the Path Cost field, specify a value (0 to 65,535) for the cost. The default depends on the port speed and link type:
   - 1000 Mbps, full duplex aggregate link (port group) — 19
   - 1000 Mbps, full duplex — 4
   - 100 Mbps, full duplex aggregate link (port group) — 19
   - 100 Mbps, full duplex — 18
   - 100 Mbps, half duplex — 19
   - 10 Mbps, full duplex aggregate link (port group) — 19
   - 10 Mbps, full duplex — 95
   - 10 Mbps, half duplex — 100
   Specify 0 to use the default cost for the port based on link speed.

5. To enable port fast convergence, select the Port Fast checkbox. Port fast convergence bypasses both the listening and learning stages and immediately places a port in the forwarding state. Use port fast convergence on network ports that are directly connected to servers, hosts, or other MAC stations.

   Informational Note:
   Do not use port fast convergence on ports connected to other bridges.
Configuring IGMP for VLANs

Internet Group Management Protocol (IGMP) snooping controls multicast traffic on a WLC by forwarding packets for a multicast group only on the ports that are connected to members of the group. IGMP is especially useful for VLANs because bandwidth is relatively constrained. The WLC listens for multicast packets and maintains a table of multicast groups, as well as their sources and receivers, based on the traffic. IGMP snooping is enabled by default.

You can configure IGMP snooping parameters and enable or disable the feature on an individual VLAN basis. The current software version supports IGMP versions 1 and 2.

To configure IGMP snooping:

1. Access the VLAN table:
   a. Select the Configuration Navigation Bar button.
   b. In the Organizer panel, click the plus sign next to a WLC.
   c. Click the plus sign next to System.
   d. Select VLANs.
2. Access the VLAN Properties multi-tabbed dialog box, then click on the IGMP tab.
3. To enable IGMP snooping, select Enable. To disable IGMP snooping, clear Enable. By default, IGMP snooping is enabled.
4. From the Version list, select Version 1 or Version 2 of IGMP.
5. If IGMP queriers are not on the subnet (for example, multicast routers), select Querier Enabled. You should use the pseudo-querier only when a VLAN contains local multicast traffic that is not routed.
6. In the Query Interval field, specify the interval (1 to 65,535 seconds) at which the WLC sends general IGMP queries on behalf of multicast routers to advertise multicast groups. The default interval is 125 seconds.
7. In the Other Querier Present Interval field, specify how long (1 to 65,535 seconds) the WLC waits for a general query to arrive before making itself the querier. The default interval is 255 seconds.
8. In the Query Response Interval field, specify how long (1 to 65,535 tenths of a second) a device can take to respond to an IGMP query. The default interval is 100 tenths of a second (10 seconds).
9. In the Last Member Query Interval field, specify how long (1 to 65,535 tenths of a second) the WLC waits for a response to a group query, after receiving a leave message for that group, before removing the group. The default value is 10 tenths of a second (1 second).
10. In the Robustness Value field, specify the robustness value (2 to 255), which sets IGMP timers to adjust to the amount of traffic loss on the network. Set the robustness value higher to adjust for more traffic loss. The default is 2.
11. To enable proxy reporting, which summarizes collected station IGMP reports, select Proxy Report.
12. To enable multicast router solicitation, which allows an MX to discover multicast routers on the subnet, select **Multicast Router Solicitation**.

13. In the **Solicitation Interval** field, specify the interval (1 to 65,535 seconds) between multicast router solicitations by a WLC. The default interval is 30 seconds.

14. Click **OK**.
Configuring Static Multicast Ports

A WLC learns about multicast routers and receivers from multicast traffic received from those devices. When the WLC receives traffic from a multicast router or receiver, the WLC adds the port that received the traffic as a multicast router or receiver port. The WLC forwards traffic to multicast routers only on the multicast router ports and forwards traffic to multicast receivers only on the multicast receiver ports.

The router and receiver ports that the WLC learns based on multicast traffic age out if they are unused. If necessary, you can statically configure multicast router ports or multicast receiver ports on the WLC.

You can only add network ports as static multicast router ports or multicast receiver ports. Ports you add are immediately added to the list and do not age out.

Informational Note:

You cannot add MP ports or wired authentication ports as static multicast ports. However, MSS can dynamically add these port types to the list of multicast ports based on multicast traffic.

To add or remove static multicast router and receiver ports:

1. Access the VLAN table:
   a. Select the Configuration Navigation Bar button.
   b. In the Organizer panel, click the plus sign next to an WLC.
   c. Click the plus sign next to System.
   d. Select VLANs.
2. In the Content panel, select a VLAN.
3. Click Properties.
4. Access the VLAN Properties multi-tabbed dialog box, then click on the VLAN Member Details tab.
5. To add a static multicast receiver port, select the Forward Multicast IP Out checkbox for each port you want to add. By default, ports are not selected. To remove a static multicast receiver port, clear the checkbox.
6. To add a multicast router port, click in the Multicast Router Present checkbox for each port you want added. By default, ports are not selected. To remove a static multicast receiver port, clear the checkbox.

Click OK.
Restricting Layer 2 Traffic Among Clients in a VLAN

By default, clients within a VLAN are able to communicate with one another directly at Layer 2. You can enhance network security by restricting Layer 2 forwarding among clients in the same VLAN. When you restrict Layer 2 forwarding in a VLAN, MSS allows Layer 2 forwarding only between a client and a set of MAC addresses, generally the default routers (gateways) of a VLAN.

Clients within the VLAN are not permitted to communicate among themselves directly. To communicate with another client, the client must use one of the specified default routers. You can specify up to four default router MAC addresses. The addresses must be unicast (not multicast or broadcast).

Informational Note:
For networks with IP-only clients, you can restrict client-to-client forwarding using ACLs. Use the Restrict L3 Traffic option.

1. Access the VLAN table:
   a. Select the Configuration Navigation Bar button.
   b. In the Organizer panel, click the plus sign next to a WLC.
   c. Click the plus sign next to System.
   d. Select VLANs.
2. In the Content panel, select a VLAN.
3. Access the VLAN Properties multi-tabbed dialog box, then click on the VLAN L2Restriction tab.
4. Select Restrict L2 Traffic to enable the feature for a VLAN.
5. Click Create.
6. In the MAC Address field, edit the address to be the MAC address of the default router (gateway) of a VLAN.
7. Click Finish.
IPSec is a general purpose Internet security protocol, and can be used for protecting Layer 4 network protocols including both TCP and UDP. IPSEc has an advantage over SSL and other methods because the application does not have to be designed to use IPSEc like other higher-layer protocols that must be incorporated into the design of an application.

To configure IP Security Destinations, follow these steps:

1. In the Task List, under Setup, click **IP Security Destinations**. This displays the **IP Security Destination** wizard.
2. To enable IP Security Destinations, select **Enable**.
3. In the **Destination** field, enter the IP address of the interface.
4. Enter a value for the **SPI**.
5. Select the type of **Encryption Algorithm**, either 3DES-CBC (less secure) or AES-CBC (more secure).
6. Enter the **Encryption Key** value. The default value is none, and you can use up to 24 hexadecimal characters.
7. Select **HMAC-SHA1** as the **Authentication Algorithm**.
8. Enter the **Authentication** Key. The default is none, but you can use up to 20 hexadecimal characters.
9. Click **OK** to save the configuration.
Restricting Layer 3 Traffic Among Clients in a VLAN

To restrict Layer 3 traffic among clients in the same VLAN, use an ACL. You can configure the ACL yourself or use the Restrict L3 Traffic option in RingMaster.

1. Access the VLAN table:
   a. Select the Configuration Navigation Bar button.
   b. In the Organizer panel, click the plus sign next to an MX.
   c. Click the plus sign next to System.
   d. Select VLANs.
2. In the Content panel, select a VLAN.
3. In the Tasks panel, select Restrict L3 Traffic.
4. Type the IP address of the default router (gateway) of a VLAN. Click Next.
5. The configured ACL block L3 traffic and is displayed. Click Finish.
Configuring the DHCP Server

MSS has a DHCP server that the WLC uses to allocate IP addresses to the following components. DHCP service for these items is enabled by default.

- Directly connected APs
- Host connected to a new (unconfigured) WLC2, WLC8, WLC200, or WLC216, to configure the WLC using the Web Quick Start

 Optionally, you can configure the DHCP server to also provide IP addresses to Distributed APs and to clients.

Caution:

Use of the MSS DHCP server to allocate client addresses is intended for temporary, demonstration deployments and not for production networks. We recommend you do not use the MSS DHCP server to allocate client addresses in a production network.

To enable the MSS DHCP server on a VLAN:

1. Access the VLAN table:
   a. Select the Configuration Navigation Bar button.
   b. In the Organizer panel, click the plus sign next to a WLC.
   c. Click the plus sign next to System.
   d. Select VLANs.
2. In the Content panel, select a VLAN.
3. Click Properties.
4. Access the VLAN Properties multi-tabbed dialog box, then click on the DHCP Server tab.
5. Select DHCP Server to enable it on a VLAN.
6. To change the range of addresses available to a DHCP server, edit addresses in the Start IP Addresses and Stop IP Addresses fields. By default, all addresses except the host address of the VLAN, the network broadcast address, and the subnet broadcast address are included in the range. If you specify the range, the start address must be lower than the stop address, and all addresses must be in the same subnet. The IP interface of the VLAN must be within the same subnet but is not required to be within the range.
7. In the Primary DNS IP Address field, enter the IP address of the primary DNS server for clients who receive addresses from this VLAN.
8. To provide a backup DNS server, type the serverIP address in the Secondary DNS IP Address field.
9. To specify the DNS domain name for hosts who receive IP addresses from this VLAN, enter the domain name in the DNS Name field.
10. To specify the default router (gateway) for hosts who receive IP addresses from this VLAN, enter the address in the Default Gateway IP Address field. Click OK.
Changing the Aging Time for FDB Entries

The aging timeout period specifies how long a dynamic entry can remain inactive before the MSS removes the entry from the database.

1. Access the VLAN table:
   a. Select the Configuration Navigation Bar button.
   b. In the Organizer panel, click the plus sign next to an MX.
   c. Click the plus sign next to System.
   d. Select VLANs.

2. In the Content panel, select a VLAN.

3. Click Properties

4. In the Aging Time field, specify the aging timeout period (0 to 1,000,000 seconds) for dynamic entries in the forwarding database. The default is 300 seconds (5 minutes). If you specify 0, aging is disabled. Click OK.
Overview of Access Control Lists (ACLs)

Access Control Lists (ACLs) filter packets to restrict or permit network usage by certain users, network devices, or traffic types. You can also assign a Class of Service (CoS) level, which allows priority handling, to packets. For example, you can use ACLs to enable users to send and receive packets within an Intranet, but restrict incoming packets to the server that stores confidential salary information.

An ACL is an ordered list of Access Control Entries (ACEs) — rules that specify how to handle packets. A rule includes a filter and an action. When a packet matches a filter, a specific action is applied to the packet. If there are no ACE matches in an ACL, it contains an implicit rule that denies all access. If there is not at least one ACE that permits access in an ACL, no traffic is allowed. The implicit "deny all" rule is always the last ACE of an ACL.

You can choose to count the number of times an ACE is matched. This hit count is useful for troubleshooting complex ACL configurations and for monitoring traffic load for specific network applications or protocols. The hit count can only be seen from the CLI. To start updating hit counter statistics in the CLI, you must first set the hits sampling rate to a nonzero value, such as 15 seconds.

You cannot perform ACL functions that include permitting, denying, or marking with a Class of Service (CoS) level on packets with a multicast or broadcast destination address.

MAC-based ACLs

Access Control Lists (ACLs) filter packets based on certain fields in the packet such as ICMP, IP address, TCP, CoS or UDP. You can also configure ACLs using MAC addresses. The MAC address mask is similar to IP address masks, but specified in hexadecimal format.

IPv6 ACLs

IPv6 addresses can also be used for creating ACLs based on IP addresses. Configuring IPv6 addresses is not supported, but IPv6 clients are supported. The WLC can view IPv6 session information and control IPv6 ACLs. The session information now includes:

- IPv6 information of both dual-stack and IPv6 only clients.
- 16 of the most recent IPv6 addresses plus one local link address of a client.

For dual stack clients, the IPv4 session is kept for storing IPv6 addresses.

IPv6 and ACLs

Previously, MSS only supported Layer 2 ACLs for IPv6. This has expanded with the release of MSS 8.0 to support:

- Source IPv6 addresses
- Destination IPv6 addresses
- Port
- Types including ICMP, TCP, and UDP

The IPv6 ACLs are differentiated from IPv4 ACLs by using the keyword, ipv6.
Creating an Access Control List (ACL)

The Create ACL wizard enables you to configure ACEs with the following parameters:

- Match criteria:
  - Source IP address
  - Destination IP address
  - Protocol?Source protocol port
  - Destination protocol port
  - Differentiated Services Code Point (DSCP) value or Type Of Service (TOS) and IP Precedence values
  - Action: deny or permit
  - Marking: Class of Service (CoS) value

These parameters are sufficient for most ACEs. To configure additional parameters, use the wizard to configure the basic parameters, then select the ACE and click Properties. (See Configuring Advanced ACL Settings.)

1. From the Organizer panel, select a WLC.
2. Under System, select ACLs.
3. Under Create, click Create ACL.
4. Enter a unique name for the ACL.
   In the ACL Name field, type the name for the ACL (1 to 32 alphanumeric characters, with no spaces or tabs). The name can include hyphens (-), underscores (_), or periods (.). ACL names are case-sensitive and must begin with a letter. Do not include any of the following terms in the name: all, default-action, map, help, editbuffer.

Informational Note:
Any ACL that refers to a DAP can be configured on the seed only as it references domain configuration. ACLs with mappings to ports, vports, and VLANs can be defined at member WLCs as well. If an ACL with the same name is defined in both the domain configuration and on a member WLC local configuration, the ACL from the WLC configuration is applied.

Adding a MAC Based Rule
To add a MAC based rule, follow these steps:
5. Click Add MAC Based Rule. The MAC Based Rules list is populated with default values.
6. To change the Source MAC from the default value of Any, click the arrow to display Source MAC Details. From the Source MAC Name list, select from Any or Other. If you select Other, enter the MAC address in the Source MAC Address field. Click OK.
7. Repeat Step 6 for the Destination MAC field.
8. To change the Ethertype, click the arrow to display Ethertype Details. From the Ethertype name list, you can select from Any, ARP, IPv4, IPv6, or Other. Click OK to close the window.
9. Select Permit or Deny from the Action list.

10. Adjust the CoS value if necessary.

11. If you have multiple rules configured, you can adjust the rule placement in the list by using the arrows at the end of each row to move the rule up or down in the list.

12. To delete a rule, select it from the list and click Delete.

**Adding an IP Based Rule**

To add an IP based rule, follow these steps:

13. Click Add IP Based Rule.

**Informational Note:**

Each ACL has a rule at the end that denies all source and destination IP addresses. This rule provides security by ensuring that the only traffic permitted by an ACL is the traffic you want to permit. This rule is automatically added to the end of each ACL and cannot be edited or removed.

After adding an ACE to the table, each subsequent ACE appears above the implicit deny all ACE at the bottom of the list, but beneath all of the other configured ACEs. An WLC uses ACEs in the order in which they appear in the list, beginning at the top. Because the action in the first ACE that matches a packet is used, the order in which ACEs are listed is important.

14. The list is automatically populated with default values.

15. To add a Source IP or Destination IP, select the field and enter the IP addresses with subnet masks.

16. To change the Protocol, click the arrow to display Protocol Details information. From the Protocol Name list, select from any, tcp, udp, icmp, svp, or other. If you select other, adjust the Protocol Number accordingly.

<table>
<thead>
<tr>
<th>IP Protocol Number</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internet Control Message Protocol (ICAP)</td>
</tr>
<tr>
<td>2</td>
<td>Internet Group Management Protocol (IGAP)</td>
</tr>
<tr>
<td>6</td>
<td>Transmission Control Protocol (TCP)</td>
</tr>
<tr>
<td>9</td>
<td>Any private interior gateway (Used by Cisco Internet Gateway Protocol)</td>
</tr>
<tr>
<td>17</td>
<td>User Datagram Protocol (UDP)</td>
</tr>
<tr>
<td>41</td>
<td>IPv6</td>
</tr>
<tr>
<td>46</td>
<td>Reservation Protocol (RSVP)</td>
</tr>
<tr>
<td>47</td>
<td>Generic Routing Encapsulation (GRE)</td>
</tr>
<tr>
<td>50</td>
<td>Encapsulation Security Payload for IPSec (IPSec-ESP)</td>
</tr>
<tr>
<td>51</td>
<td>Authentication Header for IPSec (IPSec-AH)</td>
</tr>
</tbody>
</table>
17. To specify the TCP or UDP source port: Click the down arrow in the Source Port column.

18. Select the comparison operator from the Operator pull-down list:
   - Less Than
   - Greater Than
   - Equal
   - Not Equal
   - Range
   - None (no comparison is required)

19. Select the well-known port name from the Port Name list. If the name is not in the list, select Other and type or select a port number in the Port Number field.

20. If you selected Range as the comparison operator, type or select the ending port number of the range in the Range End field. The number must be higher than the port number in the Port Number field.

21. Specify the TCP or UDP destination source port. The options are the same as those for the source port.

22. To match based on DSCP value or IP TOS and IP precedence values:
   a. Click on the down arrow in the DSCP column.
   b. Select Type Of Service or Diff-Serv Code Point.

23. If you selected Type Of Service, select the IP precedence value from the Precedence list.
   - Any (-1) . All packets are subject to the ACL regardless of whether precedence is set.
   - Routine (0) . Packets with routine precedence are filtered.
   - Priority (1) . Packets with priority precedence are filtered.
   - Immediate (2) . Packets with immediate precedence are filtered.
   - Flash (3) . Packets with flash precedence are filtered.
   - Flash Override (4) . Packets with flash override precedence are filtered.
   - CRITIC/ECP (5) . Packets with critical precedence are filtered.
   - Internetwork Control (6) . Packets with internetwork control precedence are filtered.
   - Network Control (7) . Packets with network control precedence are filtered.
24. Select the ToS value in the TOS field.
   - -1 (any) . All packets are subject to the ACE regardless of whether TOS is set.
   - 0 (normal) . Packets with normal TOS defined are filtered.
   - 1 (minimum monetary cost) . Packets with minimum monetary cost TOS defined are filtered.
25. 2 (maximum reliability) . Packets with maximum reliability TOS defined are filtered.
26. 4 (maximum throughput) . Packets with maximum throughput TOS defined are filtered.
27. 8 (minimum delay) . Packets with minimum delay TOS defined are filtered.
   By default, the TOS value is -1 (any).
28. In addition to these specific values, you can specify a number from 1 to 15 that is the sum of TOS option values. For example, to select minimum delay and maximum throughput as the TOS options, type 12, which is the sum of the two values.
29. Select the action from the Action list:
   - Permit — Allows access if the conditions in the ACE are matched
   - Deny — Refuses access if the conditions in the ACE are matched
30. To mark the packet with a CoS value, select a value in the CoS field.

Table 1: CoS Values

<table>
<thead>
<tr>
<th>Packet Priority Desired</th>
<th>CoS Value</th>
<th>AP Forwarding Queue Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background</td>
<td>1 or 2</td>
<td>4</td>
</tr>
<tr>
<td>Best Effort</td>
<td>0 or 3</td>
<td>3</td>
</tr>
<tr>
<td>Video</td>
<td>4 or 5</td>
<td>2</td>
</tr>
<tr>
<td>Voice</td>
<td>6 or 7</td>
<td>1</td>
</tr>
</tbody>
</table>

By default, the CoS Value is -1 (any).
31. If you have multiple rules configured, you can adjust the rule placement in the list by using the arrows at the end of each row to move the rule up or down in the list.
32. Click OK to save the configuration.
33. To delete a rule, select it from the list and click Delete.
Editing an Access Control List (ACL) Rules for an Existing Rule

1. From the Organizer panel, select a WLC.
2. Under System, select ACLs.
3. Select an ACL from the ACL Rules list.
4. Under Setup, click ACL Rules for "rulename" where rulename is a previously configured ACL.
5. Follow the steps in Create ACL to change the configuration.
Editing an Access Control List (ACL) Hit Sample Rate

1. From the Organizer panel, select a WLC.
2. Under System, select ACLs.
3. Under Other, click Edit ACL Hit Sample Rate.
4. Adjust the Hit Sample Rate in seconds for access rules hits. Leaving the value at 0 disables the sampling rate. You can select from a range of 0 (disabled) to 100 seconds.
5. Click OK to save the configuration.
Mapping an ACL

An ACL does not take effect until you map it to a user or an interface. You can map ACLs to ports (or port groups), VLANs, or virtual ports. You cannot map an ACL to an AP port or a wired authentication port. You can map ACLs to users by configuring the `filter.in` and `filter.out` user attributes. User-based ACLs are more specific than ACLs applied to interfaces and are therefore processed first.

1. From the Organizer panel, select a WLC.
2. Under System, select ACLs.
3. Select an ACL from the ACL Rules list.
4. Under Setup, click ACL Rules for "rulename" where rulename is a previously configured ACL.
5. Click ACL Mappings for “rulename”.
6. Select the mapping type:
   - To map to a physical port, select port and go to step 5.
   - To map to a virtual port, select vport and go to step 6.
   - To map to a VLAN, select vlan and go to step 7.
   - To map to a Distributed AP, select distributed ap and go to step 8.

Mapping an ACL to a Port

7. To map an ACL to a port:
   a. In the Port list, select a port or port group to which you want to map the ACL. You cannot map an ACL to an AP port or a wired authentication port.
   b. In the Direction list, select In to filter incoming packets or Out to filter outgoing packets.
8. Click Finish.

Mapping an ACL to a Virtual Port

9. To map an ACL to a virtual port:
   a. In the Tag Value field, specify the 802.1Q tag value that identifies a virtual port in a VLAN. The tag value can be a number from 1 to 4093. The default value is 1. Make sure that you do not specify duplicate mappings that specify the same port and tag value.
   b. In the Port list, select the port to which you want to map the ACL. You cannot map an ACL to an AP port or a wired authentication port.
   c. In the Direction list, select In to filter incoming packets or Out to filter outgoing packets.

Mapping an ACL to a VLAN

10. To map an ACL to a VLAN:
    a. In the Type list, select ID to identify the VLAN by number or Name to identify it by name.
    b. If you selected Name, select or type the VLAN name from the Name list.
    c. If you selected ID, select or type the VLAN number in the ID field.
Mapping ACL to a Distributed AP

11. To map an ACL to a Distributed AP:
   a. In the AP ID list, select a Distributed AP.
   b. In the Direction list, select In to filter incoming packets or Out to filter outgoing packets.
Configuring Advanced ACL Settings

After configuring an ACL, configure the following advanced settings:

- Hit counter (enable or disable)
- Hit sample rate (applies if the hit counter is enabled)
- Established option, to apply a new TCP ACE only to established (existing) TCP sessions. By default, TCP ACEs apply to new sessions as well as existing ones.
- ICAP properties, to specify the type and code values for ICAP ports (applies only to ACEs that have ICAP as the protocol)
- Capture option, to redirect matching packets to the CPU (applies to ACEs used for Web Portal access)

Hit Sample Rate

The hit sample rate specifies the time interval, in seconds, at which the packet counter is sampled for each security ACE on which the hit counter is enabled. By default, the hit sample rate is 0, even when the hit counter is enabled. To use the hit counter, you must enable it and set the hit sample rate. The hit sample rate applies globally to all ACEs on which the hit counter is enabled.

To change the hit sample rate:

1. From the Organizer panel, select a WLC.
2. Under System, select ACLs.
3. Under Other, click Edit ACL Hit Sample Rate.
4. Adjust the Hit Sample Rate in seconds for access rules hits. Leaving the value at 0 disables the sampling rate. You can select from a range of 0 (disabled) to 100 seconds.
5. You can enable the hit counter on an individual ACE basis. To enable the hit counter for an ACE:
   a. Select the ACE in the ACL table.
   b. In the Tasks panel, select Enable Hits for this rule.

By default, a new TCP ACE applies to new sessions as well as established (existing) sessions. To apply the ACE only to established sessions, enable the established option.

To enable the established option for TCP ACEs:

1. Select a TCP ACE in the ACL table.
2. In the Tasks panel, select Enable Established Connections.

To specify the type and code for ICAP ACEs:

Select a ICAP ACE in the ACL table.

1. In the Tasks panel, select ICAP Properties.
2. Select or type the ICAP message type in the Type field. Select or type the ICAP message code in the Code field.
3. Click OK.

Table 1: ICAP Messages

<table>
<thead>
<tr>
<th>ICAP Message (Type Number)</th>
<th>Code (Number)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Echo Reply (0)</td>
<td>None</td>
</tr>
<tr>
<td>Destination Unreachable (3)</td>
<td>• Network Unreachable (0)</td>
</tr>
<tr>
<td></td>
<td>• Host Unreachable (1)</td>
</tr>
<tr>
<td></td>
<td>• Protocol Unreachable (2)</td>
</tr>
<tr>
<td></td>
<td>• Port Unreachable (3)</td>
</tr>
<tr>
<td></td>
<td>• Fragmentation Needed (4)</td>
</tr>
<tr>
<td></td>
<td>• Source Route Failed (5)</td>
</tr>
<tr>
<td>Source Quench (4)</td>
<td>None</td>
</tr>
<tr>
<td>Redirect (5)</td>
<td>• Network Redirect (0)</td>
</tr>
<tr>
<td></td>
<td>• Host Redirect (1)</td>
</tr>
<tr>
<td></td>
<td>• TOS and Network Redirect (2)</td>
</tr>
<tr>
<td></td>
<td>• TOS and Host Redirect</td>
</tr>
<tr>
<td>Echo (8)</td>
<td>None</td>
</tr>
<tr>
<td>Time Exceeded (11)</td>
<td>• TTL Exceeded</td>
</tr>
<tr>
<td></td>
<td>• Fragment Reassembly Time Exceeded (1)</td>
</tr>
<tr>
<td>Parameter Problem (12)</td>
<td>None</td>
</tr>
<tr>
<td>Timestamp (13)</td>
<td>None</td>
</tr>
<tr>
<td>Timestamp Reply (14)</td>
<td>None</td>
</tr>
<tr>
<td>Information Request (15)</td>
<td>None</td>
</tr>
<tr>
<td>Information Reply (16)</td>
<td>None</td>
</tr>
</tbody>
</table>

4. Click OK to save the configuration.

If an ACE has the capture option, you can disable the option by selecting the ACE, then selecting Disable Capture for this rule in the Tasks panel.
Deleting an ACL

1. From the Organizer panel, select a WLC.
2. Under System, select ACLs.
3. Select an ACE in an ACL that you want to delete.
4. In the Tasks panel, click Delete.
5. Verify the selection and click Finish.

Deleting an Individual ACE from an ACL

1. From the Organizer panel, select a WLC.
2. Under System, select ACLs.
3. Select an ACE in an ACL that you want to delete.
4. In the Tasks panel, click Delete.
5. Verify the selection and click Finish.
Creating a Quality of Service (QoS) Profile

1. From the Organizer panel, select a WLC.
2. Under System, select QoS.
3. In the Tasks panel, click Create QoS Profile.
4. Enter a QoS Profile Name and click Next.

Sessions QoS Profile Settings
5. You can use the checkbox to enforce and select a bandwidth limit, and to enable and assign a value to a CoS value. To enable static CoS, select Enable Static CoS. To enable DSCP for upstream packet classification, select Trust Client DSCP.
6. Click Next.

Flow-based QoS Profile Settings
7. Enable SIP Awareness by selecting voip-data from the Traffic Class list.
   Integrated SIP awareness in a wireless network adds a new level of intelligence that allows granular and dynamic control of voice applications between wireless, wired infrastructure, and wireless handsets as well as wireless clients in the area of security and system resource management.
   8. You can use the checkbox to enforce and select a bandwidth limit, and to enable and assign a value to a CoS value. To enable static CoS, select Enable Static CoS.
9. Click Next.

QoS Profile Mapping
You can add authorization attributes such as users, user groups, MAC user groups, or SSIDs.
10. Select a Named User from the list.
11. Select a User MAC Address.
14. Select an SSID.
15. You can also map this profile to a Location Policy by selecting Map to a Location Policy.
16. Click Next.

Location Policy Rules
17. From the list of available Location Policies, select one and click Finish. If you want to check the properties of the policy, click Properties.
Setting Up DSCP to CoS Mapping

MSS supports Layer 2 and Layer 3 classification and marking of traffic, to help provide end-to-end QoS throughout a network. QoS support includes support of Wi-Fi Multimedia (WMM), which provides wireless QoS for time-sensitive applications such as voice and video.

- QoS support is automatically enabled. WLCs and AP access points each provide QoS:
  - WLCs classify and mark traffic based on 802.1p tag value (for tagged traffic) or Differentiated Services Code Point (DSCP) value.
  - AP access points classify ingress traffic from wireless clients based on the service type value in the 802.11 header, and mark the DSCP value in the IP tunnel on which the AP forwards the user traffic to the WLC.
  - APs place traffic from an WLC to a wireless client in a forwarding queue based on the DSCP value in the tunnel carrying the traffic, then forward the traffic based on the priority.

MSS performs classification on ingress to determine the CoS value. This CoS value is used to mark the packet at the egress interface. Classification and marking performed by an WLC depend on whether the ingress interface has an 802.1p or DSCP value other than 0, and whether the egress interface is tagged or is an IP tunnel. The mappings between DSCP and CoS values are configurable.

1. From the Organizer panel, select a WLC.
2. Under System, select QoS.
3. In the Tasks panel, under Setup, click DSCP to CoS Mapping.
5. In the DSCP to CoS table, change the CoS value using the up and down arrows at the end of the row.
6. In the CoS to DSCP table, change the DSCP value using the up and down arrows at the end of the row.
7. Under Setup, you can reset the values to default values or set the DSCP to CoS range. To configure the DSCP Range, click Set DSCP to CoS Range.
8. Set the first and last DSCP value as well as the CoS value. Click Finish to save the configuration.
Wireless Services Overview

If you have a WLC in your network plan, you can configure WLC Wireless features using RingMaster. The following features are available:

- Configuring Wireless Services
- Understanding Radio Profiles
- Local Switching
- Creating APs using RingMaster
- Configuring Radio Properties
- Configuring RF Detection
- Creating RF Snoop Filters
Configuring Wireless Services

RingMaster provides wizards for configuring the following types of wireless services:

- **802.1X Service Profile** — Provides wireless access to 802.1X clients.
- **Voice Service Profile** — Provides wireless access to Voice over IP (VoIP) devices.
- **Web Portal Service Profile** — Provides wireless access to clients using a Web page.
- **Open Access Service** — Provides wireless access to clients without requiring login.
- **Mesh Service Profile** — Provides wireless services to clients without a wired AP interface.
- **Custom Service Profile** — Provides wireless access based on the options you choose. (Use this option only if none of the other options applies to the type of service you want to offer.)

### Service Profile Parameters

A service profile configures an SSID. The table below lists service profile parameters. For parameters that are assigned default values, the table also lists these.

<table>
<thead>
<tr>
<th>Service Profile Parameter</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Profile Name</td>
<td>Name of the Service Profile Note: Service Profiles must have unique names.</td>
<td>Based on the Service Profiles, the Default names are 802.1X, Voice, Web-Portal, Open Access, Mesh Service, Custom</td>
</tr>
<tr>
<td>11n</td>
<td>Configure 11n parameters</td>
<td>a-mpdu-max-length, a-msdu-max-length, frame-aggregation, mode-na, mode-ng, short-guard-interval, txbf</td>
</tr>
<tr>
<td>active-call-idle-timeout</td>
<td>Set the length of time for an active call to time out on the network after becoming idle.</td>
<td>A range of seconds from 20 - 300.</td>
</tr>
<tr>
<td>SSID Name</td>
<td>SSID name associating with clients</td>
<td>Blank - no default value</td>
</tr>
<tr>
<td>Service Profile Parameter</td>
<td>Description</td>
<td>Default Value</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SSID Type</td>
<td>Encryption setting for data:</td>
<td>Based on Service Profile:</td>
</tr>
<tr>
<td></td>
<td>• Encrypted</td>
<td>• 802.1X</td>
</tr>
<tr>
<td></td>
<td>• Clear (unencrypted)</td>
<td>• Voice — Encrypted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Web-Portal — Clear</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Open — Clear</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Custom — Clear</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Mesh — Encrypted</td>
</tr>
<tr>
<td>Beaconing State</td>
<td>Advertisement of the SSID using beacons</td>
<td>Enabled</td>
</tr>
<tr>
<td>Bridging</td>
<td>Enable or disable bridging mode</td>
<td>Disable</td>
</tr>
<tr>
<td>Fallthru Access Type</td>
<td>Access type attempted if neither 802.1X nor MAC access are applicable to the client.</td>
<td>Based on Service Profile type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 802.1X — None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Voice — None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Web-Portal — Web Portal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Open Access — Last Resort</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Custom — Depends on the type of custom profile</td>
</tr>
<tr>
<td>Keep Initial VLAN</td>
<td>Keeps roaming users on the VLAN assigned by the WLC when the user logged onto the network.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Mesh Enabled</td>
<td>Configures the radio as part of a mesh configuration.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Load Balance Exempt</td>
<td>The radio on the AP does not participate in load balancing on the network.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Bandwidth Limit</td>
<td>Configures the amount of bandwidth for the service profile.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Backup SSID Mode</td>
<td>The service profile is used in backup mode on a remote WLA. You can configure it as disabled, outage-only, or dual mode.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Enable Backup SSID Timeout</td>
<td>Specify the length of time that the backup SSID is enabled.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Keep Clients</td>
<td>Specifies whether clients (sessions) are dropped or not during an outage period.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Service Profile Parameter</td>
<td>Description</td>
<td>Default Value</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Device Fingerprint</td>
<td>Configure device fingerprinting parameters</td>
<td>• device-detect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• device-detect-acl</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• device-detect-timeout</td>
</tr>
<tr>
<td>Enable Multicast Conversion</td>
<td>Enables multicast to unicast conversion on packets.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Custom Web Portal Login Page</td>
<td>Subdirectory path and file name of an HTML page customized for login to theSSID</td>
<td>Blank (default page with Juniper Networks Logo)</td>
</tr>
<tr>
<td>Security Modes</td>
<td>For encrypted SSIDs only, support encryption types include the following:</td>
<td>Based on the Service Profile</td>
</tr>
<tr>
<td></td>
<td>• Robust Security Network (RSN) also known as WPA2</td>
<td>• 802.X — Dynamic WEP</td>
</tr>
<tr>
<td></td>
<td>• WiFi Protected Access (WPA)</td>
<td>• Voice — Static WEP</td>
</tr>
<tr>
<td></td>
<td>• Dynamic Wired Equivalent Privacy (WEP)</td>
<td>• Web-Portal — No default</td>
</tr>
<tr>
<td></td>
<td>• Static WEP</td>
<td>• Open Access — Not default</td>
</tr>
<tr>
<td></td>
<td>Based on the Service Profile type:</td>
<td>• Mesh — RSN (WPA2)</td>
</tr>
<tr>
<td></td>
<td>Multiple cipers are now allowed in a service profile.</td>
<td>• Custom — Dynamic WEP for 802.X access; no default for other access types</td>
</tr>
<tr>
<td>Encryption Algorithms</td>
<td>For encrypted SSIDs only, the algorithms used to encrypt data when the WPA or RSN security mode is used:</td>
<td>Multiple cipers are now allowed in a service profile.</td>
</tr>
<tr>
<td></td>
<td>• Advanced Encryption Standard (AES) with Counter Mode with Cipher Block</td>
<td>• Voice — LOCAL (a RADIUS server group cannot be selected)</td>
</tr>
<tr>
<td></td>
<td>Chaining Message Authentication Code Protocol (CCAP)</td>
<td>• All others — Blank (you must select the method)</td>
</tr>
<tr>
<td></td>
<td>• Temporal Key Integrity Protocol (TKIP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• WEP with 40-bit keys</td>
<td></td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Location of user information the switch checks when authenticating and authorizing users. Can be one or more RADIUS server groups, the local database of the switch, or both.</td>
<td>• Voice — LOCAL (a RADIUS server group cannot be selected)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• All others — Blank (you must select the method)</td>
</tr>
</tbody>
</table>

Copyright © 2012, Juniper Networks, Inc.
You do not need to select values for all these parameters when you configure a service. Service Profile wizards help you configure essential parameters and assign appropriate values to the rest. Some parameters automatically set by RingMaster are not configurable using Service Profile wizards. To view all settings (except access rules) or change settings, select a service profile and click Properties.

<table>
<thead>
<tr>
<th>Service Profile Parameter</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Authorization</td>
<td>Attributes assigned to the service profile. An attribute value is used only if the attribute is not otherwise set, for example on a user group or individual user.</td>
<td>Blank (not set)</td>
</tr>
<tr>
<td>Radio Profile</td>
<td>802.11 radios and settings for them</td>
<td>Radio profile named default</td>
</tr>
<tr>
<td>VLAN</td>
<td>Assigned VLAN</td>
<td>Blank (not set)</td>
</tr>
<tr>
<td>VoIP</td>
<td>Assign VoIP parameters</td>
<td>• cac-mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cac-session</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cac-voip-call</td>
</tr>
</tbody>
</table>
## Encryption Types

The following table describes various encryption types for each type of Authentication Type:

### Table 1: Encryption Types for Each Authentication Type

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Encryption Types</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Static WEP</td>
<td>Dynamic WEP (rotating key) WPA Ciphers:</td>
</tr>
<tr>
<td></td>
<td>(shared secret)</td>
<td>CCA (AES) TKIP WEP104 WEP40 RSN (WPA/802.11</td>
</tr>
<tr>
<td>None</td>
<td>√</td>
<td>ciphers)</td>
</tr>
<tr>
<td></td>
<td>?</td>
<td>X</td>
</tr>
<tr>
<td>MAC Client Address</td>
<td>√</td>
<td>?</td>
</tr>
<tr>
<td>Web Portal</td>
<td>√</td>
<td>?</td>
</tr>
<tr>
<td>802.1X with subprotocols:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PEAP-MSCHAP-V2</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>EAP-MD5</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

**Legend**

- √ = Supported
- X = Not Supported
- ? = Possibly but not generally useful in an enterprise deployment
Configuring a 802.1X Service Profile for Wireless Access

**NOTE:** The 802.1X Service Profile wizard requires you to select one or more RADIUS server groups and does not allow you to complete the configuration without selecting one. Before you configure a 802.1X profile, a RADIUS server group must already be configured.

1. Access the **802.1X Service Profile** wizard:
   a. In the **Organizer** panel, click the plus sign next to an WLC to configure the service profile.
   b. Click on the plus sign next to **Wireless**.
   c. Select **Wireless Services**.
   d. In the **Tasks** panel, select **802.1X Service Profile**.

2. Read the description of the wizard on the first page, then click **Next**.

3. Type a service name in the **Name** field. Type a SSID name in the **SSID** field. Click **Next**.

4. Select the security standards supported by the SSID. Click **Next**.

5. The **Wireless Encryption Cipher Suites** dialog appears:
   - **AES (CCAP)** — Usually used with RSN (WPA2)
   - **TKIP** — Usually used with WPA
   - **WEP-104** — Used with dynamic WEP
   - **WEP-40** — Used with dynamic WEP
   Click **Next**.

6. Select one of the following from the **Authentication Server(s)** dialog.

7. Select one of the following from the **Authentication Server(s)** dialog.

8. Select an **EAP Type**:
   - **EAP-MD5 Offload**
   - **PEAP Offload**
   - **Local EAP-TLS**
   - **External RADIUS Server**
   If you select **PEAP**, the EAP Sub-Protocol is **MS-CHAPV2**.

9. The **Available RADIUS Server Groups** in the left column of the dialog can be added to the right column list of **Current RADIUS Server Groups** or they can be moved up, down or removed. Click **Next**.

10. To assign a default VLAN to the SSID, select a VLAN from the **VLAN Name** list.

11. VLAN and other authorization attributes can be assigned to users in the local database, on remote servers, or in the service profile of the SSID a user logs into. The VLAN selected here is used only if a VLAN attribute is not configured for a user on the RADIUS server or in the local database of a switch.

12. Click **Next**.
13. The **Optional: Local User Database** dialog is displayed. Select an existing user or click **Create** to configure a new user.

14. If you select an existing User, go to step 11. If you clicked **Create**, you next see the **User Information** dialog.

15. After selecting in the Local User Database, the optional **Device Detection** dialogue is displayed.

16. You can select from **Disable** to disable the feature. It is enabled by default. Or, **Just Detect**, which allows device detection but does not enforce any rules. Or, you can select **Enforce**, which enforces the device detection authorization rules. If you select Enforce, then you can configure the device detection timeout with a range of 1 to 60 seconds with a default value of 5 seconds. When you select enforce, the default ACL deviceacl is enabled. This ACL prevents access to the network until the device is recognized. Click **Next**.

17. The **Radio Profile Selection** dialog is displayed.

18. By default, the **default** radio profile is selected. Click **Create new Radio Profile** if you want to configure another radio profile. (link to subtask here) Select a Radio Profile and click **Next**.

19. You now see the **802.11n Attributes** dialog. Select desired modes and settings and click **Finish**.

20. The service profile appears in the **Service Profile** table in the **Content** panel.
Creating a 802.1X New User

1. Enter a user **Name**, **Password**, and select a **Password Expiration Time [Hours]** and **User Group**. Click **Next**.
3. Enter or select a **VLAN Name** and use pop-up menus to set **encryption-type** and **end-date**.
4. Click **Finish**.
Creating a Web Portal Service Profile

A Web Portal Service Profile creates a wireless service that allows users to authenticate using a Web browser. When the user attempts to connect to an SSID with this type of service profile, the user is redirected to a login page in a Web browser. After entering a username and password, the information is checked against a RADIUS server, or a local database, and access is granted or denied based on this information.

You can configure this type of profile for an encrypted or unencrypted SSID.

1. From the Organizer panel, select a WLC.
3. In the Task panel, under Create, click Web Portal Service Profile.
4. A brief description of the wizard is displayed.
5. Click Next.
6. Create a unique name to identify the profile.
7. Enter an SSID for the profile.
8. From the SSID Type list, select Encrypted (most secure) or Clear (least secure).
9. Click Next.
10. If you selected Encrypted, select the encryption type:
    - RSN (WPA2) — most secure
    - WPA — moderately secure
    - Static WEP — least secure
11. Click Next.
12. If you selected RSN or WPA, enter the preshared key or click Generate to create a new one. Click Next.
13. Select one or more of the following Wireless Encryption Cipher Suites:
    - AES (CCMP) — most secure
    - TKIP — moderately secure
    - WEP-104 — least secure
    - WEP-40 — least secure
    Click Next.
14. From the VLAN Name list, select the VLAN for Web Portal Users. Click Next.
15. A Web Portal ACL (portalacl) is created by default. This prevents users from accessing the network before completing the authentication process. At this point, you can add additional IP-based rules if you require them.
16. Click Next.
17. Select a AAA Server from the list of Available Server Groups. Click Add to move it to the Current AAA Server Groups. If there is no group configured, click Create Server Group. Click Next to continue the configuration.
18. Select a radio profile from the **Radio Profiles** list, or you can create a new one.

19. Optionally, you can select radios as members of the Service Profile. Select radio profile members and move them from Available Members to Current members with the Move button and the reverse with the Reset to Default button.

20. Click **Finish** to complete the configuration.
Creating an Avaya Voice Service Profile

Creating an Avaya VoWIP Service Profile:
1. Select Configuration on the toolbar.
2. In the Organizer panel, expand the WLC.
3. Expand Wireless, then select Wireless Services.
4. In the Tasks panel, select Voice Service Profile.
5. Click Next.
6. Change the service profile name to Voice-Avaya, and use the name Voice-Avaya for the SSID. Select Avaya from the Vendor list.
7. Click Next.
8. Select Open Access and clear the MAC Access checkbox.
9. Click Next.
10. Select WPA and clear Static WEP.
11. Click Next.
12. Leave TKIP enabled and click Next.
13. Type a passphrase from 8 to 63 characters long in the Pre-shared Key field and click Generate.
14. Click Next.
15. Type or select the name of the VLAN you want to place voice users in. For this example, use Voice-VLAN2.
16. Click Next.
17. An ACL is automatically created for this type of Voice Profile. The first rule in the ACL provides high-priority treatment of SVP traffic by marking IP protocol 119 (SVP) packets with CoS 7. The second rule permits all other traffic in the VLAN.
18. Enter the Source and Destination MAC Addresses.
19. Click Next.
20. Select a Radio Profile from the Radio Profiles list, and click Finish. A wireless profile Voice-Avaya is created and is displayed in the content panel.
Creating a Spectralink™ Voice Service Profile

Creating a Spectralink™ VoWIP Service Profile:
1. Select Configuration on the toolbar.
2. In the Organizer panel, expand the WLC.
3. Expand Wireless, then select Wireless Services.
4. In the Tasks panel, select Voice Service Profile.
5. Click Next.
6. Change the service profile name to Voice-SVP, and use the name Voice-SVP for the SSID.
   Select Spectralink from the Vendor list.
7. Click Next.
8. Select Open Access and clear MAC Access checkbox.
9. Click Next.
10. Select WPA and clear Static WEP.
11. Click Next.
12. Leave TKIP enabled and click Next.
13. Type a passphrase from 8 to 63 characters long in the Pre-shared Key field and click Generate.
14. Click Next.
15. Type or select the name of the VLAN you want to place voice users in. For this example, use VLAN2.
16. Click Next.
17. An ACL is automatically created for this type of Voice Profile. The first rule in the ACL provides high-priority treatment of SVP traffic by marking IP protocol 119 (SVP) packets with CoS 7. The second rule permits all other traffic in the VLAN.
18. Click Next.
19. Select a Radio Profile from the Radio Profiles list, and click Finish. A wireless profile Voice-SVP is created and is displayed in the content panel.
Creating an Vocera Voice Service Profile

1. Select Configuration on the toolbar.
2. In the Organizer panel, expand the WLC.
3. Expand Wireless, then select Wireless Services.
4. In the Tasks panel, select Voice Service Profile.
5. Click Next.
6. Change the service profile name to Voice-Vocera, and use the name VoceraBadges for the SSID. Select Vocera from the Vendor list.
7. Click Next.
8. Leave MAC Access enabled.
9. Click Next.
10. Leave Static WEP enabled.
11. Click Next. Specify WEP keys.
   - For each key (up to four), type the key value in the corresponding key field.
   - By default, data in unicast and multicast packets are encrypted using WEP key 1. To use another key for either type of packet, select the key number in the WEP Unicast Key Index or WEP Multicast Key Index field.
12. Click Next.
13. Type or select the name of the VLAN you want to place voice users in. For this example, use Voice-VLAN.
14. Click Next.
15. Click Create to add MAC users to the local database WLC.
   a. In the User MAC Address field, type the MAC address for the user device, using colons (:) as delimiters. You must specify all 6 bytes of the MAC address.
   b. In the MAC User Group list, select the MAC user group for the user device, if the group is already configured.
   c. In the VLAN Name field, select or type the name of the VLAN of the user device (1 to 16 alphanumeric characters, with no spaces or tabs). The WLC authorizes the user for that VLAN.
16. d. Click Next. In the attribute row you want to configure, click the Attribute Value column.
   d. Click Finish.
17. Click Next. Select RadioProfileVoic in the Radio Profiles list.
18. Click Finish.
Creating a WMM Voice Service Profile

Voice over Wireless IP (VoWIP) is a new technology, merging VoIP (Voice over IP) with 802.11 wireless LANs to create a wireless telephone system. Organizations that add VoWIP to the wireless LANs can deploy and manage voice and data over a single wireless backbone, reserving some portion of network bandwidth to support real-time voice communications. For a VoWIP service (sometimes also referred to simply as VoIP, or Voice over IP), you can configure either local or RADIUS server authentication, and add Access Lists (ACLs) to restrict user access.

The Voice Service Profile dialog tailors options based on the selected vendor. The dialog has the following vendor options:

- SpectraLink
- Avaya
- Vocera
- Other

The SpectraLink, Avaya, and Vocera options configure service for proprietary VoWIP solutions from these vendors. If you are configuring VoWIP for devices that use the Wi-Fi Multimedia (WMM) standard, or a proprietary solution other than one of the listed vendors, use the Other option.

Creating a WMM VoWIP Service Profile:
1. Select Configuration on the toolbar.
2. In the Organizer panel, expand the WLC.
3. Expand Wireless, then select Wireless Services.
4. In the Tasks panel, select Voice Service Profile.
5. Click Next.
6. Change the service profile name to Voice1, and use the name Voice1 for the SSID. Select Other from the Vendor list.
7. Click Next.
8. Select Open Access and clear MAC Access checkbox.
9. Click Next.
10. Select WPA and clear Static WEP.
11. Click Next.
12. Leave TKIP enabled and click Next.
13. Type a passphrase from 8 to 63 characters long in the Pre-shared Key field and click Generate.
14. Click Next.
15. Type or select the name of the VLAN you want to place voice users in. For this example, use VLAN2.
16. Click Next.
17. Select Enable WMM.
18. Click Next.
19. Select a Radio Profile from the Radio Profiles list and click Finish. A wireless profile Voice1 has been created and is shown in the content panel.
Creating an Open Access Service Profile

1. From the Organizer panel, select a WLC.
3. In the Task panel, under Create, click Open Access Service Profile.
4. A brief description of the wizard is displayed.
5. Click Next.
6. Create a unique name to identify the profile.
7. Enter an SSID for the profile.
8. From the SSID Type list, select Encrypted (most secure) or Clear (least secure).
9. If you selected Encrypted, select the encryption type:
   - RSN (WPA2) — most secure
   - WPA — moderately secure
   - Static WEP — least secure
10. Click Next.
11. If you selected RSN or WPA, enter the preshared key or click Generate to create a new one.
    Click New.
12. Select one or more of the following Wireless Encryption Cipher Suites:
    - AES (CCMP) — most secure
    - TKIP — moderately secure
    - WEP-104 — least secure
    - WEP-40 — least secure
    Click Next.
13. If you selected Static WEP, specify WEP keys.
    - For each key (up to four), type the key value in the corresponding key field.
    - By default, data in unicast and multicast packets are encrypted using WEP key 1. To use another key for either type of packet, select the key number in the WEP Unicast Key Index or WEP Multicast Key Index field.
14. From the VLAN Name list, select the VLAN for Open Access Users. Click Next.
15. Select a radio profile from the Radio Profiles list, or you can create a new one.
16. Click Finish to complete the configuration.
Creating an Mesh Service Profile

WLAN mesh services allow an AP to provide wireless services to clients without a wired interface on the AP. Instead of a wired interface, there is a radio link to another AP with a wired interface. WLAN mesh services can be used at sites when running Ethernet cable to a location is inconvenient, expensive or impossible. Note that power must be available at the location where the Mesh AP is installed.

1. From the Organizer panel, select a WLC.
3. In the Task panel, under Create, click Mesh Service Profile.
4. Create a unique name to identify the profile.
5. Enter an SSID for the profile.
6. If desired, Select Bridging to allow an AP to bridge wireless traffic destined for a wired network.

7. Select the type of access for this profile:
   - Authenticate APs by MAC Address (default)
   - Allow Access to any AP with a valid pre-shared key.

8. If you select authentication using a MAC address, select a MAC Address User from the list or click Create to add a new user.

9. If you select authentication using a pre-shared key, enter a preshared key in raw hexadecimal format. Or, enter a passphrase into the Preshared Key field and click Generate to obtain the hexadecimal format. You should set this key in the boot configuration of an AP.

10. Select a radio profile from the Radio Profiles list, or you can create a new one. You must have a unique radio profile for mesh services.

11. Click Finish to complete the configuration.
Creating a Custom Service Profile

If none of the other service types is appropriate, you can use the Custom Service Profile wizard to configure a service. The screens and options displayed depend on access types and elections you make as you use a wizard. All pages and options occur in at least one of the other service profile wizards.

1. From the Organizer panel, select a WLC.
3. In the Task panel, under Create, click Custom Service Profile.
4. Create a unique name to identify the profile.
5. Enter an SSID for the profile.
6. From the SSID Type list, select Encrypted (most secure) or Clear (least secure).
7. Select the type of access for this profile:
   - 802.1X Access
   - MAC Access
   - Web Access
   - Open Access
   - Click Next.
8. Select one or more wireless security standards. Click Next.
9. If you have a preshared key authenticating clients, enter it into the Preshared Key field and click Encrypt to encrypt the key. Click Next.
10. Select one or more wireless encryption suites. Click Next.
11. Select a VLAN for Open Access users.
12. Select a radio profile and click Finish to complete the configuration.
Understanding Radio Profiles

A radio profile is a set of attributes that you can apply to multiple radios. A default radio profile named default is provided and cannot be deleted. Rather than configuring each radio individually, you can create a new radio profile and apply it to multiple radios that you select. You can also create a radio profile as part of a domain policy and apply the policy to APs on different WLCs.

The default radio profile is associated with the APs of an WLC, unless you created a new radio profile while configuring the coverage area and configured the WLCs with the information in the floor plan. If you create a new radio profile while configuring a coverage area for a floor, RingMaster automatically copies the new profile to the domain policy of the Mobility Domain selected for the coverage area. Later, when you configure WLCs in the Mobility Domain using the information in the floor plan, RingMaster also copies the radio profile to the Radio Profiles policy of each of the switches.
Creating Radio Profiles

To create a Radio Profile, use the following steps:

1. In the Organizer panel, select a WLC.
3. In the Tasks panel, under Create, click Create Radio Profile.
4. Enter a unique radio profile name in the Name field.
5. Click Next.
6. Select a radio or radios from the Available Members, and click Move to add it to the Current Members.
7. Click Next to continue configuring additional options or click Finish to save the Profile.
8. Click Next.
9. Select a Service Profile to apply to the Radio Profile and click add to move it to the Current Service Profiles.
10. Click Finish to save the configuration.

Configuring Advanced Radio Settings

After configuring a radio profile, select the radio profile, and click Properties to display a series of tabs that contain all of the configurable parameters for the radio profile. You can configure the following settings:

Radio Profile
- Name — Radio profile name
- Countermeasures Mode:
  - None — Radios do not use countermeasures. This is the default.
  - Rogue and Suspect — Sends probe any requests (probe requests with a null SSID name), to solicit probe responses from other access points. Radios also passively scan by listening for beacons and probe responses. When active scan is disabled, radios perform passive scanning only.
  - Rogue — A rogue is a device that is in the Juniper network but does not belong there. An interfering device is not part of the Juniper network but also is not a rogue. MSS classifies a device as an interfering device if no client connected to the device has been detected communicating with any network entity listed in the forwarding database (FDB) of any WLC in the Mobility Domain. Although the interfering device is not connected to your network, the device might be causing RF interference with AP radios. Radios use countermeasures against devices classified by MSS as rogues, but do not use countermeasures against devices classified by MSS as interfering devices.
- Enable RFID — Enables support for RFID tags.
- Enable U-APSD — Enables Unscheduled Automatic Powersave Delivery (U-APSD) on AP radios managed by the radio profile. U-APSD enables WMM clients that use powersave mode to more efficiently request buffered unicast packets from AP radios.
• Restrict DFS Channels
• Client Tx Power Constraint

RF Scanning
• Mode
• Channel Scope
• Send CTS-to-Self
• Enable/Disable Spectral Scan — enables Spectrum Analysis on the profile.

802.11 Attributes
• Beacon Interval — Interval that the MP advertises the SSIDs. You can specify from 25 to 8191 milliseconds (ms). The default is 100 ms.
• DTIM Period — Number of beacons (1 to 31) the MP transmits before transmitting the multicast and broadcast frames stored in its buffers. The default is 1.
• Fragment Threshold (bytes) — Frame length (256 to 2346 bytes) at which the long-retry-count is applicable instead of the short-retry-count. The default is 2,346 bytes.
• Max Tx MDSU Lifetime (ms) — Maximum amount of time, from 500 ms to 250,000 ms (250 seconds), the MP can hold an outbound frame in buffer storage. The default value is 2,000 ms (2 seconds).
• Max Rx MDSU Lifetime (ms) — Maximum amount of time, from 500 ms to 250,000 ms (250 seconds), the MP can hold an inbound frame in buffer storage. The default is 2000 ms (2 seconds).
• RTS Threshold (bytes) — Minimum length (256 to 3000 bytes) a frame can be for the MP to use the Request-To-Send/Clear-To-Send (RTS/CTS) method to send the frame. Frames smaller than the RTS threshold are not sent using the RTS/CTS method. The default is 2346 bytes.
• Enable Long Preambles — Enables advertisement of long preambles for 802.11b/g radios. This option is enabled by default. This option applies only to 802.11b/g radios.
• Enable Rate Enforcement — When data rate enforcement is enabled, clients transmitting at the disabled rates are not allowed to associate with the AP. Data rate enforcement is disabled by default.

802.11n Attributes
• Channel Width
Auto Tune

- Tune Channel — Automatically configures and tunes the channel. This feature is enabled by default.

**Informational Note:**

RF Auto-Tuning of channels on 802.11a radios uses only the bottom four channels in the band (36, 40, 44, and 48.) To use a higher channel number, you must disable RF Auto-Tuning of channels on the radio profile for the radio, and statically configure the channel. However, you can only configure channels legally allowed by the country code.

The network plan configuration task Disable Auto-tune stamps current values into the permanent WLC configuration.

- Tune Transmit Power — Automatically configures and tunes the power. This feature is disabled by default.
- Ignore Clients — Select if you want the radio to deflect clients to other radios.
- Tune Channel Range (11a)
  - All bands
  - Lower bands
- Channel Tuning Interval (seconds) — Interval at which RF Auto-Tuning decides whether to change the channels on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio channels if needed. You can specify from 0 to 65535 seconds. The default channel interval is 3600 seconds. It is recommended that you use an interval of at least 300 seconds (5 minutes). If you set the interval to 0, RF Auto-Tuning does not reevaluate the channel at regular intervals. However, RF Auto-Tuning can still change the channel in response to RF anomalies.
- Tx Power Tuning Interval (seconds) — Interval at which RF Auto-Tuning decides whether to change the power level on radios. You can specify from 1 to 65535 seconds. The default is 300 seconds.
- Power Ramp Interval (seconds) — Interval at which power is increased or decreased, in 1 dBm increments, on radios until the optimum power level calculated by RF Auto-Tuning is reached. After each power ramp interval, the radio increases or decreases the power by another 1 dB until the radio reaches the power level selected by RF Auto-Tuning.
- Channel Tuning Hold Down (seconds) — Minimum number of seconds a radio in a radio profile must remain at its current channel assignment before RF Auto-Tuning can change the channel. The channel holddown provides additional stability to the network by preventing the radio from changing channels too rapidly in response to spurious RF anomalies such as short-duration channel interference. You can specify from 0 to 65535 seconds. The default channel interval is 900 seconds.
• Tx Power Backoff Timer (seconds) — Interval at which radios reduce power after temporarily increasing the power to maintain the minimum data rate for an associated client. At the end of each power-backoff interval, radios that temporarily increased their power reduce it by 1 dBm. The power backoff continues in 1 dBm increments after each interval until the power returns to expected setting. You can specify from 0 to 65535 seconds. The default is 10 seconds.

Service Profile Selection
The Profile Selection tab lists the service profiles mapped to a radio profile. Radios managed by a radio profile provide wireless service for service profile SSIDs. To map a radio profile to a service profile, select a service profile from the Available Service Profiles list. Click Add to move the profile name to the Current Service Profiles list. To remove mapping between a radio profile and a service profile, select a service profile from the Current Service Profiles list. Click Remove to move the profile name to the Available Service Profiles list.

• Available Service Profiles
• Current Service Profiles

Radio Selection
The Radio Selection tab lists the radios managed by the radio profile. A radio can be managed by only one radio profile. To add a radio to the radio profile, select the radio in the Available Members list. Click Add to move the radio to the Current Members list. To remove a radio from the radio profile, select the radio from the Current Members list. Click Reset to Default to return the radio to the default radio profile.

• Available Members
• Current Members

Voice Configuration
• QoS Mode — Classification and marking of high priority traffic on the WLC and AP
  – WMM — Classifies, marks, and forwards traffic for Wi-Fi Multimedia (WMM) devices based on 802.1p and DSCP values.
  – SVP — Optimizes forwarding of SpectraLink Voice Priority (SVP) traffic by setting the random wait time an AP radio waits before transmitting the traffic to 0 microseconds

• WMM CAC Configuration
  – Background 0 ACM Mode
  – Background 0 ACM Limit (%)
  – Background 0 ACM Policing
  – Best-effort 1 ACM Mode
  – Best-effort 1 ACM Limit (%)
  – Best-effort 1 ACM Policing
  – Video 2 ACM Mode
  – Video 2 ACM Limit (%)
  – Video 2 ACM Policing
  – Voice 3 Mode
Overview
A successful wireless LAN depends on efficient channel assignment by the WLAs. Channel assignment defines strategy of channel allocation that targets minimizing interference. Wireless interference, which causes low throughput due to collisions on the network, severely limits network capacity and can be minimized by using non-overlapping channels for neighboring WLAs.

The Adaptive Channel Planner improves radio channel assignment in the following situations:

- New deployment - no existing channel configuration using either RingMaster or manually configuring the channels on the WLCs.
- Existing configuration - improvement desired for any reason.
- Moving or adding WLAs
- Interference sources with channel-specific effects.

ACP provides better wireless connectivity to clients by dynamically assigning operating channels on WLAs. The benefits include:

- Optimizing the use of available spectrum across the entire wireless network.
- Reducing interference by avoiding medium access contention
- Maximizing channel reuse
- Avoiding performance degradation generated by spectrum overlap.
- Restoring wireless connectivity in the presence of severe interference.
- Minimize the impact of channel changes for wireless services.
- Avoiding channel changing that makes the network plan less optimal than the previous plan.
- Minimizing the impact of non-802.11 interference on the overall quality of service experience.

Functionality
Adaptive Channel Planner (ACP) dynamically assigns the WLA operating channel so that the wireless network can efficiently adapt to the RF environment conditions. Dynamic assignment can be changed when significant changes are measured in the interference level or in the network topology. Eventually, Wi-Fi bandwidth is maximized and maintains the efficiency of communication over the wireless network.
ACP is enabled by default, but you can disable it. It is also overwritten if a static channel set is configured. If ACP is not configured, channels on the WLAs are static and require manual intervention to change the channels.

Here’s how it works:

- **Measure** - MSS monitors the RF environment and collects interference information.
- **Calculate** - MSS uses the measured data to calculate the best channel to assign on the WLA. This is a background function that does not impact other functions on the WLA.
- **Deploy** - MSS changes the operational channels when it is determined to have minimal impact on connected clients.

You can configure ACP to run at periodic intervals in order to calculate the next auto channel based on a measured interference level or when network changes are detected. MSS continuously searches for better channel assignment configurations, and separately monitors and controls 802.11a and 802.11b/g networks preventing unnecessary changes to one network if the other network is impacted.

You can select from channel sets and the default channel list includes only non-overlapping channels that meet regulatory requirements. This means that different channel sets are available based on the county code used in the configuration. Because of limited availability, channels are reused. The same channel is assigned to two WLAs, located far enough apart, if the overlapping channel interference signal detected by each WLA is less than a defined threshold. However, if radar is detected on the network, the channel is not available in the channel list for 30 minutes.

To improve the scaling characteristics of ACP, a new concept called "Interference Domain" is introduced. An InDo is defined as a set of radios in a MoDo that can interfere with each other. It only exists for the duration of an ACP cycle.

If a cluster configuration is enabled on the MoDo, ACP is applicable across the entire MoDo. Otherwise, the settings are restricted to the local configuration.

To configure Adaptive Channel Planner, select a radio profile and click Properties.

1. Click on the Adaptive Channel Planner tab.
2. To add specific channels on the 802.11b/g radio, select the tab and add channels by moving them from Available Channels to Current Channels.
3. To add specific channels on the 802.11a radio, select the tab and add channels by moving them from Available Channels to Current Channels.
Setting Up Bandwidth Management

Select one or more options to manage bandwidth. You can enforce per SSID bandwidth limits, control how a radio bandwidth is shared across SSIDs, and configure QoS profiles to limit bandwidth and prioritize traffic individual users or SSIDs.

1. From the Organizer panel, select an WLC and then Wireless Services.
2. In the Tasks panel, under Setup, click Bandwidth Management.
3. All Bandwidth Management Options are selected by default. To disable an option, clear the corresponding checkbox.
4. Click Finish if you have disabled an option. To continue the configuration, click Next.
5. To configure limits for an SSID, select a Service Profile from the list.
6. Click Next.
7. To configure SSID Access Time for a radio profile, select the name from the Radio Profile Name list. To enable weighted queuing, select Enable Weighted Queuing.
8. Click Next.
9. Manage any configured QoS profiles, or create one.
10. Click Finish.
Creating a VLAN Profile

To create a VLAN Profile for Local Switching, use the following steps:

1. From the Organizer panel, select a WLC.
2. Under Wireless, select Local Switching.
3. In the Tasks panel, click Create VLAN Profile.
4. In the Name field, enter a unique name to identify the profile.
5. Click Next.
6. Select a VLAN from the Network Plan VLANs, and click Add to move it to the Current VLANs list.
7. If you do not have any VLANs configured, click Add VLAN to create a new one.
8. Click Next.
9. From the Available APs list, select APs to apply the profile. Click Move to add it to the Current APs list.
10. Click Finish to complete the configuration.
Setting Up L2 Restrictions for Local Switching

To set up L2 Restrictions for Local Switching, use the following steps:

1. From the Organizer panel, select a WLC.
2. Under Wireless, select Local Switching.
3. In the Tasks panel, under Setup, select L2 Restrictions.
4. From the VLANs list, select an available VLAN.
5. Click Next.
6. To enable L2 Traffic Restrictions on the VLAN, select Enable.
7. If there are no restrictions configured, click Create.
8. Enter a MAC address to use for the configuration, and click Finish.
9. Select the MAC address from the list, and click Finish.
Creating APs using RingMaster

To add APs, use the following steps:

1. In the Organizer panel, select a WLC.
3. In the Tasks panel, under Create, click AP.
4. Create a unique identity for the AP. Enter a number, unique name, connection type, and description. Click Next.
5. Enter the AP serial number in the Serial Number field. If you plan to configure security between the AP and an WLC, enter the unique fingerprint for the AP.
6. Click Next.
7. Select the AP type from the AP Model list. The Radio 1 Type and Radio 2 Type are automatically populated when you select the AP Model.
8. Click Next.
9. Configure the Radio 1 parameters:
   - Number
   - Radio Mode
   - Radio Profile
   - Channel Number
   - Transmit Power [dBm]
   - Antenna Location
   - Antenna Type
10. Click Next.
11. Configure the Radio 2 parameters:
   - Number
   - Radio Mode
   - Radio Profile
   - Channel Number
   - Transmit Power [dBm]
   - Antenna Location
   - Antenna Type
12. Click Finish to save the configuration.
Managing Access Points Using RingMaster

If you currently have access points in a RingMaster plan, use these steps to change the configuration:

1. From the Organizer panel, select a WLC.
2. Under **Wireless**, select **Access Points**.
3. In the Configuration panel, you can change the following settings:
   - **Security Mode** - select from Optional, None, or Required.
   - **Enable Auto AP**
   - **Load Balancing** - enabled by default.
4. For existing WLAs in RingMaster, you can highlight them in the list and click **Properties**.
5. You can change or add the following properties to a WLA:
   - **Access Point**
     - AP Number
     - Name
     - AP Mode
     - Description
     - Radio Type
     - Serial Number
     - Connection
     - Fingerprint
     - Location
     - Contact
     - AP Communication Timeout
     - Enable Data Security
     - Bias
     - Enable Firmware Update
     - Force Image Download
     - Enable Blink
     - LED Mode
     - Local Switching
   - **Remote AP**
     - Enable Remote AP
     - Outage Duration [hours]
     - Connection Evaluation Period [seconds]
     - High Latency Mode
- LLDP
  - LLDP Mode
  - LLDP-MED Mode
  - Power via MDI
  - Inventory
- 802.11ng Radio
  - Number
  - Radio Mode
  - Radio Profile
  - Channel Number
  - Transmit Power [dBm]
  - Antenna Location
  - Antenna Type
  - Antenna Span [degrees]
  - Antenna Direction [degrees]
  - Cable Loss [dBm]
  - Auto Tune
    - Max Transmit Power
  - Load Balancing
    - Enable Load Balancing
    - Load Balance Group
    - Rebalance Clients
- 802.11na Radio
  - Number
  - Radio Mode
  - Radio Profile
  - Channel Number
  - Transmit Power [dBm]
  - Antenna Location
  - Antenna Type
  - Antenna Span [degrees]
  - Antenna Direction [degrees]
  - Cable Loss [dBm]
  - Auto Tune
    - Max Transmit Power
- Load Balancing
  - Enable Load Balancing
  - Load Balance Group
  - Rebalance Clients
- AP Redundancy
  - Select or Create a Connection

6. Click OK to save the changes.

Deleting an Existing AP

To delete an AP from the current configuration, select the AP from the list and click Delete. The AP is removed from the configuration.
Creating an AP Number

To set up AP Number, use the following steps:
1. In the Organizer panel, select a WLC.
3. In the Tasks panel, under Setup, click AP Number.
4. Create a new and unique AP number.
5. Click OK to change the AP Number.
Setting Up AP Model

To set up APModel, use the following steps:
1. In the Organizer panel, select a WLC.
3. In the Tasks panel, under Setup, click AP Model.
4. From the AP list, select an AP model.
5. Click OK to change the AP Model.
Setting Up AP Boot Configuration

To set up AP Boot Configuration, use the following steps:

1. In the Organizer panel, select a WLC.
3. In the Tasks panel, under Setup, click AP Boot Configuration.
4. From the AP list, select an AP to apply the configuration.
5. Click Change Boot Parameters.
6. To clear the boot configuration, select Clear Configuration.
7. Under Mesh, to enable the feature, select Mesh Enabled. You can also generate a Mesh PSK and add the SSID.
8. Under IP, if the AP boots from a static IP address, select Static IP Enabled. Enter the Gateway, Static IP Address, and Netmask.
9. Under Switch, if the AP boots from a specific WLC, select Static WLC Enabled. Enter the Static IP WLC Address, Static WLC Name, and Static IP DNS Address.
10. Under VLAN, if the AP is assigned to a VLAN, select Static VLAN Enabled, and the Static VLAN Tag.
11. Click OK to add the configuration.
12. Click Next to deploy the changes.
13. Click Finish to close the wizard.
Setting Up Load Balancing

RF load balancing is the ability to reduce network congestion over an area by distributing client sessions across the WLAs with overlapping coverage in the area. When the total demand of nearby wireless clients exceeds the capacity of a single WLA, there is no interruption of wireless services on the network.

For example, in an auditorium or lecture hall, there may be a substantial number of clients in a relatively small amount of space. While a single WLA may be sufficient for providing an RF signal to the entire area, more WLAs are required to deliver enough aggregate bandwidth for all of the clients. When additional WLAs are installed in the room, RF load balancing allows the client sessions to be spread evenly across the WLAs, increasing the available aggregate bandwidth by increasing the number of WLAs.

RF load balancing is enabled by default. In addition, RF load balancing is done on a per-radio basis, rather than a per-WLA basis. For radios managed by a given radio profile, RingMaster automatically assesses radios with overlapping coverage in an area and balances the client load across them.

RingMaster balances the client load by adjusting how WLAs are perceived by clients. As the capacity of an WLA handling new clients is relative to other WLAs in the area, RingMaster makes the WLA more difficult for potential new clients to detect, which causes a client to associate with an WLA with more capacity. An WLA becomes more difficult to detect and clients then associate with an WLA with higher capacity for client sessions. By default RingMaster only prevents clients from associating with an WLA if there are other WLAs with available capacity. Clients are not prevented from associating with a WLA if it is the only one available.

You can optionally place WLA radios into load balancing groups. When two or more WLA radios are placed in the same load balancing group, RingMaster assumes that they have exactly the same coverage area, and attempts to distribute the client load across them equally. The WLA radios do not have to be on the same WLC. A balanced set of WLA radios can span multiple WLC switches in a Mobility Domain.

To set up Load Balancing, use the following steps:

1. In the Organizer panel, select a WLC.
3. In the Tasks panel, under Setup, click Load Balancing.
4. To enable Load Balancing between APs, select Load Balancing.
5. Configure the Load Balancing Strictness, by selecting from the following options:
   - Low - No clients are denied service.
   - Medium - Clients attempting to connect to overloaded APs are redirected to other APs causing a few seconds delay before connecting to the network.
   - High - Clients may be delayed up to a minute before connecting to the network.
   - Max -
6. Select the preferred bandwidth, and click Next.
7. Configure Load Balancing for each radio. You can enable the Rebalance Clients option, and click Next.

8. Select the Service Profiles to apply Load Balancing, and also select which Service Profiles are exempt from this feature.

9. Click Finish to add the configuration.
Setting Up AP Redundancy

To setup AP Redundancy, use the following steps:

1. In the Organizer panel, select a WLC.
3. In the Tasks panel, under Setup, click AP Redundancy.
4. To add an AP, click Create.
5. If you have a directly connected AP, configure the AP Connection settings:
   a. WLC - select an WLC from the list.
   b. Port
   c. Bias
   d. PoE - if you want the AP to receive power from the WLC, select this option.
6. Click Finish to add the connection.
7. If you have an AP previously configured for redundancy, you can edit the connection properties by selecting the AP, and then clicking Properties.
Setting Up AP Radio Type

To set up APRadio Type, use the following steps:

1. In the Organizer panel, select a WLC.
3. In the Tasks panel, under Setup, click AP Radio Type.
4. Select a Radio Type from the list.
5. Click OK to change the AP Radio Type.
Configuring Remote AP using RingMaster

Overview

In some network deployments, it is common to have a central network site with WLCs and remote sites with WLAs. The central and remote sites are connected by a WAN link. If the WAN link becomes unavailable, then the remote sites with WLAs remain active and continue to provide connectivity to wireless clients.

Once an outage has occurred, a periodic timer sends discovery messages to the primary access manager (PAM) to detect when the WLC is available on the network again. This timer, called an evaluation timer, is configurable and can be used as a hold-down timer to confirm detection of the WAN outage and as a mechanism to detect when the connection is restored.

A remote office can be any one of the following types of environments:

- Small retail store using the corporate database for inventory control and the Internet for financial transactions.
- Remote investment office with local servers, IP/PBX, and access to the corporate network for financial information.
- Remote sales office with access to the corporate network only.
- A temporary office at an event or exhibition with local printers and access to the corporate database across the WAN.
- A hot spot deployed at a retail facility, such as a coffee shop, providing Internet access only.
- A healthcare clinic that requires access to centralized hospital data in addition to local networking services such as printers and servers.

Once you have installed RingMaster Version 7.5 or later, you can configure WLAs for Remote AP using the following steps:

1. In the Organizer panel, select a WLC from the list and then Access Points.
2. On the Navigation bar, click Configuration.
3. Select an Access Point from the list of Access Points, and click Properties.
4. Click the Remote AP tab to display the options for configuring a Remote AP.
5. Select Enable Remote AP.
6. In the Outage Duration [hours], configure the length of time for the WLA to stay in outage mode. The default setting is 0 (stay in outage mode indefinitely) and the range is from 0 to 120 hours (5 days). This period indicates the maximum length of time that a WLA remains in outage mode.
7. In the Connection Evaluation Period [seconds], configure the length of time for the keepalive interval of the pings sent to detect when the WAN link is active on the network. The default value is 300 seconds with a range of 5 to 86400 seconds.
8. Click OK to save the changes in RingMaster.
You can also configure WAN Outage on Auto APs when you use the Auto AP wizard. Select **Enable Auto AP** on the **Access Points** Configuration panel, then click **Auto AP** under **Setup** on the **Tasks** panel.

To receive alarms about Remote APs, configure SNMPv2, and add the trap APNonOperStatus2 trap 3 to the Notification Profile. The following events occur when the WLA is in Remote AP mode:

- When a WLA changes to an outage state, an AP Status Alarm is sent with the reason Connection Lost 4.
- If the WLA recovers and exits the outage mode before the Extended Timeout expires, an AP Status Alarm is sent with reason Connection Restored 5.
- If the Extended Timeout expires, an AP Status Alarm is sent with reason Connection Outage Extended Timeout 6.

In the first two instances, the WLA stays active, but in the last instance, the WLA is down.

### Configuring a Remote Site with RingMaster

To configure a Remote Site with RingMaster, select Remote Site located in the Organizer.

Once you select **Remote Sites** in the **Organizer**, click **Create Remote Site** to launch the configuration wizard. The wizard allows you to configure the following parameters:

- Unique Name
- Country Code
- Enable Security
- VLAN Profile
- Path MTU
- Enable Backup SSIDs Mode
- Add WLAs
Converting Auto APs

To an Auto AP to a configured AP, use the following steps:

1. In the Organizer panel, select a WLC.
3. In the Tasks panel, under Other, click Convert Auto AP.
4. From the list of Auto APs, select one to convert to a configured AP, and click Next.
5. Change the AP Number to a unique number, and click Next.
6. The selected AP is converted to a configured AP.
7. Click Finish.
Removing Auto APs

To remove an Auto AP, use the following steps:

1. In the Organizer panel, select a WLC.
3. In the Tasks panel, under Other, click Remove Auto AP.
4. From the list of Auto APs, select one to remove, and click Next.
5. The selected AP is removed from the network plan.
6. Click Finish.
AAA Overview

If you have a WLC in your network plan, you can configure WLC AAA features using RingMaster. The following features can be configured:

- Creating Users in the Local Database
- Creating a RADIUS Server
- Creating a LDAP Server
- Creating AAA Profiles
- Creating an 802.1X Authentication Rule
- Creating a MAC Access Rule
- Creating a Web Authentication Rule
- Creating a Open Access Rule
- Creating an Admin Access Rule
- Creating a Console Access Rule
- Creating RADIUS Proxy Client
- Creating a Location Policy Rule
- Creating a Mobility Profile
- Configuring Device Fingerprinting
Creating a RADIUS Server

To add a RADIUS Server to RingMaster, use the following steps:

1. From the Organizer pane, select a WLC.
2. Under AAA, select RADIUS.
3. In the Task Panel, under Create, click Create RADIUS Server.
4. Enter a name to identify the RADIUS Server.
5. Enter the IP address in the IP Address field.
6. Enter the authentication key in the Key field.
7. To use the MAC address as the password, select Use MAC as Password.
8. Enter the Authorization password.
9. If you are using the MAC address as the password, select the format from the MAC Address Format list.
10. Create a RADIUS Server Group for the RADIUS server. A RADIUS Server Group can contain multiple RADIUS servers and allows you to create redundancy and load balancing for AAA.
11. Click Next.
12. Since the RADIUS Server Group was created in the previous step, the server group appears in the list of Current RADIUS Server Groups.
13. Click Finish to complete the configuration.
Creating a RADIUS Server Group

To create a RADIUS Server Group, use the following steps:

1. From the Organizer pane, select a WLC.
2. Under AAA, select RADIUS.
3. In the Tasks panel, under Create, click Create RADIUS Server Group.
4. Enter a name to identify the RADIUS Server Group.
5. Select one or more RADIUS Servers to be member of the RADIUS Server Group. Click Add to move them to the list of Current RADIUS Servers.
6. To allow load balancing between servers, select Load Balance.
7. Click Finish to complete the configuration.
To enable RADIUS Accounting, use the following steps:

1. From the Organizer pane, select a WLC.
2. Under AAA, select RADIUS.
3. In the Task Panel, under Setup, click System Accounting.
4. Select a RADIUS Server or multiple RADIUS servers from the Available AAA Server Groups, and click Add. The server is moved to the Current AAA Server Groups. As you add servers, you can also change the order that they appear in the list. Use the Up and Down arrows to change the server order in the list.
5. Select Enabled under RADIUS Accounting.
6. Click OK to complete the configuration.
Creating a RADIUS Dynamic Authorization Client (DAC)

To create a RADIUS DAC, use the following steps:
1. From the Organizer pane, select a WLC.
2. Under AAA, select RADIUS.
3. In the Tasks panel, under Create, click Create RADIUS DAC.
4. Enter a name to identify the RADIUS DAC.
5. Enter the IP Address of the RADIUS DAC.
6. Enter the authentication key.
7. Click Next.
8. To apply a Wired Access Rule, enable it by selecting Wired Access Rule.
9. Select the SSIDs that the RADIUS DAC can modify connection properties and authorization attributes. Select Any to allow the RADIUS DAC to modify any SSID.
10. Click Add to add the SSID to the list of Associated SSIDs.
11. Click Finish.
Setting Up RADIUS Defaults

You can specify default settings that apply to all RADIUS servers configured on a WLC. You can also specify RADIUS DAC settings that apply to all DACs connecting to the RADIUS DAC server.

To configure default RADIUS settings, use the following steps:

1. From the Organizer pane, select a WLC.
2. Under AAA, select RADIUS.
3. In the Task Panel, under Setup, click RADIUS Defaults.
4. The following default settings can be configured:
   - Timeout [seconds] — The range is from 1 to 65535 seconds with a default value of 5 seconds.
   - Retry Count — Specify how many times that a RADISU request is retried on the RADIUS server. The range is 1 to 100 with a default value of 3.
   - Dead Time [minutes] — Specify how long to wait after a RADIUS server times out. The range is 0 to 1440 minutes with a default value of 5 minutes.
   - Key — Enter the authentication key used to communicate with the RADIUS server.
   - Use MAC as Password — Use the MAC address of the server as the password.
   - Authorization Password — Enter the default authorization password for the server.
   - MAC Address Format — Select the MAC address format for the server. You can select one of the following options:
     - None
     - Hyphens
     - Colons
     - One Hyphen
     - Raw
   - Authentication Protocol — Select the Authentication Protocol for the server. You can select one of the following options:
     - PAP
     - CHAP
     - MSCHAP-V2
   - RADIUS DAS Port — Configure the port for the Dynamic Authentication Server. The default value is 3799.
5. Click OK to complete the configuration.
Configuring Command Audit Properties

To enable RADIUS Accounting, use the following steps:

1. From the Organizer pane, select a WLC.
2. Under AAA, select RADIUS.
3. In the Task Panel, under Setup, click Command Audit.
4. Select the Log level to record the command audit trail. You can select from None, Default, or All.
5. Configure the log file size by selecting the number of kilobytes from the list. Once the maximum is reached, the log begins to overwrite the existing file. The minimum is 200 KB with a maximum of 2000 KB. The default value is 500 KB.
6. Click Next.
7. Select a RADIUS Server Group from the list of Available AAA Server Groups. Click Add to move it to the list of Current AAA Server Groups. You can reorder the servers in the list by using the Up and Down arrows. Once you add the server to the Current AAA Server Group list, Command Accounting is automatically enabled.
8. Click Finish to complete the configuration.
Configuring CDR Accounting Properties

To enable CDR Accounting, use the following steps:

1. From the Organizer pane, select a WLC.
2. Under AAA, select RADIUS.
3. In the Task Panel, under Setup, click CDR Accounting.
4. Select a RADIUS Server Group from the list of Available AAA Server Groups. Click Add to move it to the list of Current AAA Server Groups. You can reorder the servers in the list by using the Up and Down arrows. Once you add the server to the Current AAA Server Group list, CDR Accounting is automatically enabled.
5. Click OK to complete the configuration.
Configuring RADIUS Ping

RingMaster provides a RADIUS ping utility to enhance troubleshooting capabilities if there are problems communicating with a RADIUS server. The radping command allows an WLC to send an authentication request to a RADIUS server to determine if that server is active or offline. You must authenticate on the RADIUS server using MSCHAPv2 authentication.

To configure RADIUS Ping, use the following steps:

1. From the Organizer panel, select a WLC.
2. Under AAA, select RADIUS.
3. In the Task Panel, under Other, click RADIUS Ping.
4. You can configure the following RADIUS Ping command parameters:
   - **Target** — Select a RADIUS Server from the list of servers.
   - **Request Type** — Select one of the following Request Types:
     - **Authentication** — requires a username and password.
     - **Start Accounting** — Begin collecting statistics for user accounts on the server.
     - **Stop Accounting** — Stop collecting statistics for user accounts on the server.
     - **Update Accounting** — Update the accounting statistics.
     - **Accounting On** — Enable accounting statistics collection on the server.
     - **Accounting Off** — Enable accounting statistics collection on the server.
5. Enter the **Username** and **Password** to authenticate on the RADIUS Server.
6. Click **Start**.
7. The ping information is displayed in the **Status** panel.
8. Click **Stop** to end the session.

Configuring Split Authentication and Authorization

With the implementation of RADIUS Ping, a RADIUS server authenticates a user but authorization attributes are received from the WLC local user database. This is accomplished by including a Vendor-Specific Attribute (VSA) in the RADIUS Accept response. When the WLC receives the RADIUS Accept response, the WLC uses the group name and attempts to match it to authorization attributes of a corresponding user group in the local user database.

To configure this feature, additional attributes must be configured on the RADIUS server. For the user-group name, specify a string consisting of 1-32 characters. Additional values consist of Type - 26, Vendor ID - 14525, Vendor Type - 9 (Trapeze VSA).

**Informational Note:**

The VSA value remains Trapeze until it is converted to Juniper in the next release of MSS and RingMaster.
Attributes that appear in the RAIDUS Accept response are added to the session attributes. If the Access Accept has a Trapeze group-name VSA, the attributes from the corresponding user group in the local database are applied.
Configuring SmartPass Servers for AAA

This wizard assists you with configuring SmartPass servers for Authentication, Accounting, Dynamic Authorization, and CDR Accounting. You can also configure a SmartPass server as an External Captive Portal.

To configure a SmartPass Server for AAA, use the following steps:

1. From the Organizer pane, select a WLC.
2. Under AAA, select RADIUS.
3. In the Task Panel, under Setup, click SmartPass.
4. After reading the description of the feature, click Next.
5. From the list of Available SmartPass Servers, select one and click Add to move it to the list of Current SmartPass Servers.
6. Click Next.
7. Configure the SmartPass RADIUS Server Group by selecting an available AAA Server from the list. Click Add to move it to the list of Current RADIUS Servers. If you want to load balance network traffic between the servers, select Load Balance.
8. Select the options from the SmartPass Options list to add to the configuration. You can select from the following options:
   - Authentication
   - Accounting
   - Dynamic Authorization
   - CDR Accounting
9. Click Next.
10. Select an existing Service Profile, either 802.1X or Web Portal. You can also create a new one by selecting Create New Service Profile. (Link to service profile information)
11. To edit the properties of an existing profile, select it from the list of Service Profiles and click Properties. (Link to Service Profile Type)
12. Click Next.
13. To configure Accounting options, select the SSIDs and the corresponding Access Rules are automatically created.
14. If you select RADIUS DAC, you can configure the RADIUS Server as Self or the SmartPass server.
15. Select Configure as DAC if you want the server to act as a Dynamic Client.
16. Select a SSID from the list of Available SSIDs and click Add to move it to the Associated SSIDs.
17. Click Next.
18. To configure the CDR Accounting options, select the SmartPass server group from the list of Available AAA Server Groups and click Add to move it to the list of Current AAA Server Groups.

19. Click Finish to complete the configuration.
Creating a LDAP Server

To create a LDAP Server, use the following steps:

1. In the Organizer panel, select a WLC.
2. Under AAA, click LDAP Server.
3. From the Tasks panel, click Create LDAP Server.
4. Enter a unique name for the LDAP Server.
5. Enter the IP Address of the server.
6. Enter the Fully Qualified Domain Name (FQDN) of the LDAP server.
7. Click Next.
8. An LDAP Server Group is automatically created with the name of the LDAP Server.
9. Click Next.
10. The LDAP Server Group appears in the list of Current LDAP Server Groups. If you want to remove it from the server group, select it and click Remove.
11. Click Finish to complete the configuration.

Changing LDAP Server Properties

To change any of the LDAP Server properties, select it from the list of servers and click Properties. Change the desired options, and click OK to complete the configuration. You can change the following options:

- **IP Address**
- **Timeout [seconds]** - Sets the timeout for communication with the LDAP server. You can set the time in seconds with a range of 1 to 65535 seconds. The default value is 5 seconds.
- **Authentication Port** - The default port is 389.
- **Dead Time [minutes]** - The length of time to wait before recontacting a LDAP server. The range is 0 to 1440 minutes with a default value of 5 minutes.
- **Bind Mode** - Select from NONE, SIMPLE-AUTH, SASL-MD5.
- **MAC Address Format** - Select from None, Hyphens, Colons, One Hyphen, or Raw.
- **Base DN**
- **Prefix DN**

Deleting a LDAP Server

To delete any of the LDAP Servers, select it from the list of servers and click Delete. Click Finish to confirm that you want to delete the server.
Creating a LDAP Server Group

To create a LDAP Server Group, use the following steps:
1. In the Organizer panel, select a WLC.
2. Under AAA, click Create LDAP Server Group.
3. Enter a unique name for the LDAP Server Group.
4. Select one or more LDAP Servers to add to the group.
5. Click Add to move the servers to the Current LDAP Servers list. You can change the order of the servers by using the Up and Down arrows.
6. Click Finish to complete the configuration.

Changing LDAP Server Group Properties

To change the LDAP Server Group properties, select it from the list of LDAP Server Groups, and click Properties. You can change the following properties:
- Load Balancing
- Adding or Removing LDAP Servers from the LDAP Server Group.

Deleting a LDAP Server Group

To delete any of the LDAP Server Groups, select it from the list of servers and click Delete. Click Finish to confirm that you want to delete the server group.
Configuring LDAP Default Settings

To create a LDAP Server Group, use the following steps:

1. In the Organizer panel, select a WLC.
2. Under AAA, select LDAP.
3. In the Tasks panel, under Setup, click LDAP Defaults.
4. You can change the following default settings
   - Timeout [seconds] - Sets the timeout for communication with the LDAP server. You can set the time in seconds with a range of 1 to 65535 seconds. The default value is 5 seconds.
   - Authentication Port - The default port is 389.
   - Dead Time [minutes] - The length of time to wait before recontacting a LDAP server. The range is 0 to 1440 minutes with a default value of 5 minutes.
   - Bind Mode - Select from NONE, SIMPLE-AUTH, SASL-MD5.
   - MAC Address Format - Select from Hyphens, Colons, One Hyphen, or Raw.
   - Fully Qualified Domain Name (FQDN) - the domain name for the LDAP Server.
   - Base DN -
   - Prefix DN -
5. Click OK to complete the configuration.
Configuring 802.1X Global Parameters

802.1X Access Rules include information about the Extensible Authentication Protocol (EAP) type to use for AAA communication between the client and the AAA server. The EAP type can be one of the following:

- **EAP-MD5 Offload** — EAP with Message-Digest (algorithm)5 (MD5). Select this protocol for wired clients.
  - Uses challenge-response to compare hashes.
- **Dynamic Authorization Server Port** — the UDP where the DAS listens for Disconnect and CoA requests sent by the DAC.

To configure 802.1X global parameters, use the following steps:

1. In the Organizer panel, select a WLC.
2. Under AAA, click 802.1X.
3. In the 802.1X section, you can configure the following parameters:

**802.1X**

- **System Authentication Control** — To enable 802.1X authentication for all wired authentication ports on the WLC, select System Authentication Control. To disable 802.1X authentication for all wired authentication ports, clear System Authentication Control. By default, 802.1X authentication is enabled.

- **Retransmit Timeout [seconds]** — To specify the number of seconds before retransmitting an Extensible Authentication Protocol over LAN (EAPoL) packet, specify the timeout value (1 to 65,535 seconds) in the Retransmit Timeout field. The default is 5 seconds.

- **Authentication Server Timeout [seconds]** — To specify the number of seconds before timing out a request to an authentication server, specify the timeout value (1 to 65,535 seconds) in the Authentication Server Timeout field. The default is 30 seconds.

- **Key Transmit** — To enable encryption key information to be sent to the client after authentication in EAPoL-Key PDUs, select Key Transmit. The WLC sends EAPoL key messages after successfully authenticating the client and receiving authorization attributes for the client. If the client is using dynamic WEP, the EAPoL key messages are sent immediately after authorization. To disable this option, clear Key Transmit. By default, this option is enabled.

- **Reauthentication Attempts** — To specify the number of reauthentication requests before a client becomes unauthorized, specify the value (1 to 10) in the Reauthentication Attempts field. The default is 2 attempts.

- **Bonded Period [seconds]** — To specify the number of seconds MSS retains session information for Bonded Auth™ (bonded authentication), specify the value, from 1 to 300 seconds, in the Bonded Period field. The default is 0 seconds.

- **Quiet Period Timeout [seconds]** — To specify the number of seconds before attempting reauthentication, specify the timeout value (0 to 65,535 seconds) in the Quiet Period Timeout field. The default is 60 seconds.
• **Supplicant Timeout [seconds]** — To specify the number of seconds before timing out an authentication session with an 802.1X client (supplicant), specify the timeout value (1 to 65,535 seconds) in the Supplicant Timeout field. The default is 30 seconds.

• **Maximum Requests** — To set the maximum number of times an EAP request is transmitted to the client before timing out the authentication session, specify the value (0 to 10) in the Maximum Requests field. The default is 2 attempts.

  **Informational Note:**
  To support SSIDs that have both 802.1X and static WEP clients, MSS sends a maximum of two ID requests, even if this parameter is set to a higher value. Setting the parameter to a higher value does affect all other types of EAP messages.

• **Reauthentication** — To enable reauthentication of 802.1X clients, select Reauthentication. To disable reauthentication, clear Reauthentication. By default, reauthentication is enabled.

  **Informational Note:**
  If the number of reauthentications for a wired authentication client is greater than the maximum number of reauthentications allowed, MSS sends an EAP failure packet to the client and removes the client from the network. However, MSS does not remove a wireless client from the network under these circumstances.

• **Reauthentication Period [seconds]** — To specify the number of seconds before reauthentication is attempted, specify the timeout value, from 60 to 1,641,600 seconds (19 days), in the Reauthentication Period field. The default is 3600 seconds (one hour). MSS re-authenticates dynamic WEP clients based on a re-authentication timer. MSS also re-authenticates WPA clients if they use WEP-40 or WEP-104 cipher. For each dynamic WEP client or WPA client using a WEP cipher, the reauthentication timer is set to the lesser of the global setting or the value returned by the AAA server with the rest of the authorization attributes for that client.

• **Handshake Timeout [msecs]** — Set the handshake timeout period. You can enter a value in milliseconds from 20 to 5000. The default value is 2000 milliseconds.

**WEP Key Rolling**

• **WEP Key Rolling** — To enable WEP key rolling (rotation) of the broadcast and multicast WEP keys, select WEP Key Rolling.

• **WEP Key Rolling Period [seconds]** — To specify the time to wait before rotating the WEP key, specify the value, from 30 to 1,641,600 seconds, (19 days) in the WEP Key Rolling Period field. The default is 1800 seconds (30 minutes).

**TKIP/CCMP Key Rolling**

To maintain secure wireless access to the network, keys used to encrypt packets should be difficult to guess or hack by a third party.
• Adding the option to enable or disable unicast periodic rekeying with a configurable interval value. When the timer expires, the client unicast key (PTK) is changed when a 4-way handshake is initiated.

• Adding the option to enable multicast periodic rekeying with a configurable interval value. When the timer expires, all VLAN keys (GTK) is changed by initiating a 4-way or 2-way handshake.

• **Unicast Key Rolling** — select to enable Unicast Key Rolling.

• **Unicast Key Rolling Period [seconds]** — Configure a value from 30 to 86400 seconds. The default value is 300 seconds.

• **Multicast Key Rolling** — select to enable Multicast Key Rolling.

• **Multicast Key Rolling [seconds]** — Configure a value from 30 to 86400 seconds. The default value is 300 seconds.
Creating AAA Profiles

To configure AAA Profiles, use the following steps:

1. In the Organizer panel, select a WLC.
2. Under AAA, click AAA Profiles.
3. In the Tasks panel, under Create, click Create AAA Profile.
4. Enter a unique name to identify the profile.
5. Click Next.
6. You can add, modify, or create Access Rules associated with this profile.

Creating an Access Rule

7. Click Create. You can create one of the following types of Access Rules:
   - 802.1X Authentication Rule (x-ref to configuring this type of rule)
   - MAC Authentication Rule
   - Web Authentication Rule
8. Click Finish to complete the configuration.

If you want to modify the Access Rule, select the Rule and then click Properties. Edit any of the available parameters and click OK.

You can reorder the rules in the list using the Up and Down arrows.
Creating AAA Profile Access

To configure AAA Profile Access, use the following steps:

1. In the Organizer panel, select a WLC.
2. Under AAA, click AAA Profiles.
3. In the Tasks panel, under Create, click Create AAA Profile Access.
4. From the SSID list, select a SSID to apply the access rule. If the rule applies to Wired Auth users, select Wired Auth.
5. Select an AAA Profile from the list.
6. Click Next.

Optional: Accounting Servers

7. To enable accounting for the profile, select Enabled.
8. From the Record Type list, select from the following options:
   - Start-Stop
   - Start-Only
9. From the list of Available AAA Server Groups, select one from the list and click Add to move it to the list of Current AAA Server Groups. You can reorder the server groups in the list by using the Up and Down arrows.
10. Click Finish to complete the configuration.
Overview of Access Rules

Service Profile wizards create network access rules to control access to the SSIDs configured by each wizard. Access rules match on all usernames or MAC addresses for voice service profiles. Table 1 lists the access rules automatically created by the service profile wizards.

Table 1: Access Rules Created Automatically by Service Profile Type

<table>
<thead>
<tr>
<th>Service Profile Type</th>
<th>Access Rule Type</th>
<th>Default Access Glob</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X</td>
<td>802.1X</td>
<td>**</td>
</tr>
<tr>
<td>Voice</td>
<td>MAC</td>
<td>*</td>
</tr>
<tr>
<td>Mesh</td>
<td>MAC</td>
<td>*</td>
</tr>
<tr>
<td>Web-Portal (WebAAA)</td>
<td>Web</td>
<td>**</td>
</tr>
<tr>
<td>Custom</td>
<td>Can be one or more of the above, depending on the type of Service Profile.</td>
<td>None. No access rules are configured automatically. You must configure them as part of the wizard steps.</td>
</tr>
</tbody>
</table>

The ** and * values are wildcards. The ** wildcard matches on all usernames. To match on all MAC addresses, use only a single *.

You can restrict access by specifying part of the username or MAC address along with a wildcard *. In this case, only the usernames or MAC addresses that match the partial username or address are allowed access to the network.

User Globs and MAC Address Globs

A user glob is a string containing wildcards that matches on one or more usernames. The format of a user glob depends on the client type and Extensible Authentication Protocol (EAP) method.

- For Windows® domain clients using Protected EAP (PEAP), the user glob is in the format Windows_domain_name\username. The Windows domain name is the NetBIOS domain name and must be specified in capital letters. For example, EXAMPLE\sydney, or EXAMPLE\*.*, which specifies that all users with usernames containing a period are allowed access.

- For EAP with Transport Layer Security (EAP-TLS) clients, the format is username@domain.name. For example, sydney@example.com specifies the user sydney in the domain name example.com. The *@marketing.example.com specifies all users in the marketing department in example.com. The user glob sydney@engineering.example.com specifies the user sydney in the engineering department at example.com.

For a MAC address glob, type a full or partial username to be matched during authentication. MAC addresses must be specified with colons as the delimiters, for example, 00:12:34:56:78. You can use wildcards by specifying an asterisk (*) in MAC addresses.

The following lists examples of using wildcards in MAC addresses:
- * (all MAC addresses)
- 00:*
- 00:01:*
- 00:01:02*
- 00:01:02:03:*
- 00:01:02:03:04:*
- 00:01:02:03:04::0*
Creating an 802.1X Authentication Rule

To configure an 802.1X Access Rule, use the following steps.

1. From the Organizer panel, select a WLC.
2. Select AAA, and the 802.1X Access Rules.
3. From the Tasks panel, under Create, select 802.1X Access Rule.
4. Select a SSID from the SSID list.
5. If the rule applies to a Wired Auth user, select Wired.
6. In the Matching User Glob field, enter specific usernames or "***" to match all usernames.
7. Click Next.

EAP Type

8. Select the EAP Type from the list. You can select from the following options:
   - External Authentication Server — No protocol is used by the WLC. Mobility System Software (MSS) sends the EAP processing to a RADIUS server. If you select PEAP, the EAP Sub-Protocol is MS-CHAPV2. For other protocols, there is no EAP Sub-Protocol to select.
   - EAP-MD5 Offload — Extensible Authentication Protocol (EAP) with message-digest algorithm 5. Select this protocol for wired authentication clients.
     - Uses challenge-response to compare hashes.
     - Provides no encryption or integrity checking for the connection.
     - Uses TLS for encryption and data integrity checking.
     - Provides MS-CHAP-V2 mutual authentication.
     - Only the server side of the connection needs a certificate.
   - Local EAP-TLS — EAP with TLS.
     - Provides mutual authentication, integrity-protected negotiation, and key exchange.
     - Requires X.509 public key certificates on both sides of the connection.
     - Provides encryption and integrity checking for the connection.
     - Cannot be used with RADIUS server authentication (requires user information to be in the local database of the WLC).
9. If you selected PEAP as the EAP type, MS-CHAPV2 is selected by default as the EAP Sub-Protocol.
10. Click Next.

Authentication Servers

11. To enable authentication, select Enabled.
12. Select a server group from the list of Available AAA Server Groups, and click Add to move it to the list of Current AAA Server Groups. You can reorder the list by using the Up and Down arrows.

   If you select Local, you are adding the local database on the WLC.

13. Click Next.

Optional: Accounting Servers

14. To enable accounting for the profile, select Enabled.

15. From the Record Type list, select from the following options:
   - Start-Stop
   - Stop-Only

16. From the list of Available AAA Server Groups, select one from the list and click Add to move it to the list of Current AAA Server Groups. You can reorder the server groups in the list by using the Up and Down arrows.

17. Click OK to complete the configuration.
Creating a MAC Access Rule

To create a MAC Access Rule, use the following steps:

1. From the Organizer panel, select a WLC.
3. In the Tasks panel, under Create, click MAC Network Access.
4. Select a SSID from the SSID list.
5. If the rule applies to a Wired Auth user, select Wired.
6. In the Matching MAC Address Glob field, you can either specify a user MAC address or a MAC Address Glob up to 5 bytes long ending with ":*" to match specific MAC addresses or "*" to match all MAC addresses.
7. Click Next.

**Authentication Servers**

8. To enable authentication, select Enabled.
9. To use the MAC Address Prefix, select MAC Prefix.
10. Select a server group from the list of Available AAA Server Groups, and click Add to move it to the list of Current AAA Server Groups. You can reorder the list by using the Up and Down arrows.
    
    If you select Local, you are adding the local database on the WLC. MAC Authentication allows you to select from RADIUS or LDAP servers.

**Optional: Accounting Servers**

11. To enable accounting for the profile, select Enabled.
12. From the Record Type list, select from the following options:
    - Start-Stop
    - Stop-Only
13. From the list of Available AAA Server Groups, select one from the list and click Add to move it to the list of Current AAA Server Groups. You can reorder the server groups in the list by using the Up and Down arrows.
14. Click Finish to complete the configuration.
Creating a Web Authentication Rule

To configure a Web Access Rule, use the following steps.

1. From the Organizer panel, select a WLC.
3. From the Tasks panel, under Create, select Web Access Rule.
4. Select a SSID from the SSID list.
5. If the rule applies to a Wired Auth user, select Wired.
6. In the Matching User Glob field, enter specific usernames or "***" to match all usernames.
7. Click Next.
8. Select a server group from the list of Available AAA Server Groups, and click Add to move it to the list of Current AAA Server Groups. You can reorder the list by using the Up and Down arrows.

If you select Local, you are adding the local database on the WLC. MAC Authentication allows you to select from RADIUS or LDAP servers.

Optional: Accounting Servers

9. To enable accounting for the profile, select Enabled.
10. From the Record Type list, select from the following options:
    • Start-Stop
    • Stop-Only
11. From the list of Available AAA Server Groups, select one from the list and click Add to move it to the list of Current AAA Server Groups. You can reorder the server groups in the list by using the Up and Down arrows.
12. Click Finish to complete the configuration.
Creating a Open Access Rule

To configure an Open Access Rule, use the following steps.
1. From the Organizer panel, select a WLC.
2. Select AAA, and then Open Access Rules.
3. From the Tasks panel, under Create, select Open Access Rule.
4. Select a SSID from the SSID list.
5. If the rule applies to a Wired Auth user, select Wired.
6. Click Next.

Optional: Accounting Servers
7. To enable accounting for the profile, select Enabled.
8. From the Record Type list, select from the following options:
   - Start-Stop
   - Stop-Only
9. From the list of Available AAA Server Groups, select one from the list and click Add to move it to the list of Current AAA Server Groups. You can reorder the server groups in the list by using the Up and Down arrows.
   - Click OK to complete the configuration.
10. Click Finish to complete the configuration.
Creating an Admin Access Rule

To configure an Admin Access Rule, use the following steps.

1. From the Organizer panel, select a WLC.
2. Select AAA, and then Admin Access Rules.
3. From the Tasks panel, under Create, select Create Admin Access.
4. Create and enter a User Glob for the Admin User Name.
5. Click Next.
6. Select an Authentication Server from the list of Available AAA Server Groups and click Add to add it to the list of Current AAA Server Groups.
7. Click Next.

Optional: Accounting Servers

8. To enable accounting for the profile, select Enabled.
9. From the Record Type list, select from the following options:
   - Start-Stop
   - Stop-Only
10. From the list of Available AAA Server Groups, select one from the list and click Add to move it to the list of Current AAA Server Groups. You can reorder the server groups in the list by using the Up and Down arrows.
11. Click Finish to complete the configuration.
Creating a Console Access Rule

To configure a Console Access Rule, use the following steps.
1. From the Organizer panel, select a WLC.
2. Select AAA, and then Admin Access Rules.
3. From the Tasks panel, under Create, select Console Access.
4. In the Matching User Glob field, enter specific usernames or "***" to match all usernames.
5. To enable authentication, select Enabled.
6. Select a server group from the list of Available AAA Server Groups, and click Add to move it to the list of Current AAA Server Groups. You can reorder the list by using the Up and Down arrows.
   If you select Local, you are adding the local database on the WLC.
7. Click Next.

Optional: Accounting Servers
8. To enable accounting for the profile, select Enabled.
9. From the Record Type list, select from the following options:
   - Start-Stop
   - Stop-Only
10. From the list of Available AAA Server Groups, select one from the list and click Add to move it to the list of Current AAA Server Groups. You can reorder the server groups in the list by using the Up and Down arrows.
11. Click OK to complete the configuration.
Creating RADIUS Proxy Client

To create RADIUS Proxy Client, use the following steps.

1. From the Organizer panel, select a WLC.
2. Select AAA, and then RADIUS Proxy.
3. From the Tasks panel, under Create, select RADIUS Proxy Client.
4. Enter the IP address of the RADIUS client (third party AP).

Optional: RADIUS Messaging Ports

You can enter the UDP ports where the WLCs listens for RADIUS access-requests and stop-accounting records. You can leave Authentication Port and Accounting Port at the default values.

5. Click Next.
6. Enter the Client Key for authenticating and encrypting RADIUS communication.
7. Click Finish.
Creating Proxy Access

To configure Proxy Access, use the following steps.

1. From the Organizer panel, select a WLC.
2. Select AAA, and then RADIUS Proxy.
3. From the Tasks panel, under Create, select Proxy Access.
4. In the Matching User Glob field, enter specific usernames or "***" to match all usernames.
5. To enable authentication, select Enabled.
6. Select a server group from the list of Available AAA Server Groups, and click Add to move it to the list of Current AAA Server Groups. You can reorder the list by using the Up and Down arrows.
   If you select Local, you are adding the local database on the WLC.
7. Click Next.

Optional: RADIUS Server Group

8. From the list of Available AAA Server Groups, select one from the list and click Add to move it to the list of Current AAA Server Groups. You can reorder the server groups in the list by using the Up and Down arrows.
   If you select Local, you are adding the local database on the WLC.
9. Click Finish to complete the configuration.
Creating 802.1Q Mappings

To create 802.1Q Mappings, use the following steps.

1. From the Organizer panel, select a WLC.
2. Select AAA, and then RADUIS Proxy.
3. From the Tasks panel, under Create, select 802.1Q Mappings.
4. Select a Port.
5. Enter the SSID.
6. Create a unique tag for the mapping.
7. Click OK.
Creating a Location Policy Rule

To configure a Location Policy Rule, use the following steps.

1. From the Organizer panel, select a WLC.
2. Select AAA, and then Location Policy.
3. From the Tasks panel, under Create, select Create Location Policy Rule.
4. Configure the Location Rule Match Option. You can select from the following options:
   - SSID
   - User Glob
   - VLAN
   - Time of Day
   - Port List
   - DAP List
5. For each of the listed options, select the values to use for the Location Policy. Click Next.

Optional: Port Criteria
6. Select a physical port to apply the location policy. Click Next.

Optional: Distributed APs Criteria
7. Select from a distributed AP from the list of Available Distributed APs, and click Add to put it in the Current Distributed APs list.
8. Click Next.

Location Rule Action
9. Configure the Location Rule to allow or deny access to the network. If access is allowed you can override authorization attributes by specifying new values. You can configure the following parameters:
   - Action
   - In ACL
   - Out ACL
   - VLAN Name
   - Time of Day Action
   - URL
   - QoS Profile
   - Termination Action
10. Click Finish to complete the configuration.
Creating a Mobility Profile

To configure a Location Policy Rule, use the following steps.

1. From the Organizer panel, select a WLC.
2. Select AAA, and then Mobility Profiles.
3. From the Tasks panel, under Create, select Create Mobility Profile.
4. Create a unique name for the Mobility Profile.

Optional: Mobility Profile Port Selection

5. Select a physical port from the list of Available Physical Ports, and click Add to put it in the Current Physical Ports list.

6. Click Next.

Optional: Distributed APs Criteria

7. Select from a distributed AP from the list of Available Distributed APs, and click Add to put it in the Current Distributed APs list.

8. Click Finish.
Configuring Device Fingerprinting

DHCP Fingerprinting Overview

This feature supports the ability of MSS to detect the type of device used by a client when authenticating on the wireless LAN. Devices include iPads, iPhones, Windows PC, tablets, etc. This feature implements the DHCP fingerprinting method.

What is a DHCP Fingerprint?

A DHCP fingerprint is almost a unique identifier for a specific operating system or device type. Due to the broadcast and pervasive nature of DHCP, DHCP fingerprinting provides a low cost and minimal effort method of passive system identification and inventory. MSS examines the DHCP message from various devices and identifies unique characteristics for each device. This information is used to compile a fingerprint database which is then used to identify the device type for clients as they join the network.

When a mobile device attempts to connect to the wireless network, it sends a DHCP Discover packet in an attempt to locate a DHCP server on the network. This is a “conversation starter” between the device and the DHCP server.

The second phase of the conversation is the return of a DHCP Offer packet from the DHCP server to the mobile device. After reserving an IP address for the client, the DHCP server sends a DHCP Offer packet with the client MAC address, the IP Address, lease duration, and the IP address of the DHCP server sending the Offer packet.

In the third phase, the mobile client returns a DHCP Request packet to the DHCP server accepting the IP address.

And in the final fourth phase, the DHCP Server sends a DHCP Acknowledgement packet with the lease duration and any other information requested by the mobile device client.

The Role of DHCP in Device Fingerprinting
When a DHCP client of an operating system sends a DHCP request Discover or Request), the request contains DHCP options such as DNS server, WINS server, or default gateway, and the WLA looks for DHCP options. The option order is relatively unique and identifies the specific operating system version. Option 55, Parameter Request List, contains the options requested by the client. The DHCP Discover or Request packet is inspected for Option 55, and the option list is matched against the database to determine the client type. DHCP Option 55 is not unique and the same parameters may be sent by different clients. In this case, other DHCP options are inspected by MSS.

Figure 1: An example of a DHCP Packet Exchange

In the diagram, you can see the different DHCP Options that are communicated during the process. Once the DHCP Discover information is exchanged, a DHCP Request packet is sent from the mobile device.
In addition, there are differences between an initial DHCP request packet and a DHCP Request packet sent after a mobile device “wakes up”.

![Figure 2: An Example of a DHCP Request Packet](image)

If a mobile device receives the information it needs to connect to the network, and successfully connects, it retains the information for the active session. If the device “goes to sleep”, and then “wakes up”, it sends a DHCP Request packet asking if the initial information is still available. If it is, the mobile device reconnects using that information.

**Table 1: Common DHCP Options**

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Host Name</td>
<td>minimum of 1 octet</td>
</tr>
<tr>
<td>50</td>
<td>Requested IP address</td>
<td>4 octets</td>
</tr>
<tr>
<td>51</td>
<td>IP Address Lease Time</td>
<td>4 octets</td>
</tr>
<tr>
<td>53</td>
<td>DHCP Message Type</td>
<td>1 octet</td>
</tr>
<tr>
<td>54</td>
<td>Server Identifier</td>
<td>4 octets</td>
</tr>
<tr>
<td>55</td>
<td>Parameter Request List</td>
<td>minimum of 1 octet</td>
</tr>
<tr>
<td>57</td>
<td>Maximum DHCP Message Size</td>
<td>2 octets</td>
</tr>
<tr>
<td>58</td>
<td>Renewal (T1) Time Value</td>
<td>4 octets</td>
</tr>
<tr>
<td>60</td>
<td>Vendor class identifier</td>
<td>minimum of 1 octet</td>
</tr>
<tr>
<td>61</td>
<td>Client-identifier</td>
<td>minimum of 2 octets</td>
</tr>
<tr>
<td>81</td>
<td>FQDN Option</td>
<td>1 octet</td>
</tr>
</tbody>
</table>
Option 55 Parameter Request List

It is possible to configure device fingerprint rules based on the Parameter Request List in DHCP Option 55. You can put them in the order of priority but the DHCP server may not process them specifically in the requested order. The table lists DHCP Option 55 parameters:

<table>
<thead>
<tr>
<th>Parameter Number</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Subnet Mask</td>
</tr>
<tr>
<td>2</td>
<td>Time Offset</td>
</tr>
<tr>
<td>3</td>
<td>Router</td>
</tr>
<tr>
<td>6</td>
<td>Domain Name Server</td>
</tr>
<tr>
<td>31</td>
<td>Perform Router Discover</td>
</tr>
<tr>
<td>33</td>
<td>Static Route</td>
</tr>
<tr>
<td>43</td>
<td>Vendor-specific information</td>
</tr>
<tr>
<td>44</td>
<td>NetBIOS over TCP/IP Server</td>
</tr>
<tr>
<td>47</td>
<td>NetBIOS over TCP/IP Node Type</td>
</tr>
<tr>
<td>78</td>
<td>Directory Agent Information</td>
</tr>
<tr>
<td>79</td>
<td>Service Location Agent Scope</td>
</tr>
<tr>
<td>95</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>112</td>
<td>NetInfo Parent Server Address</td>
</tr>
<tr>
<td>113</td>
<td>NetInfo Parent Server Tag</td>
</tr>
<tr>
<td>249</td>
<td>Classless Static Route</td>
</tr>
<tr>
<td>252</td>
<td>Proxy autodiscovery</td>
</tr>
</tbody>
</table>

When a device attempts to join the wireless LAN, information is gathered from the device and matched against the fingerprint database to identify the device type. Once the device type is detected, that information is used to apply policies or report information useful to the network administrator.

**Informational Note:**

The WLA captures the device fingerprint information and sends it to the WLC to determine policy enforcement.

Also, when the WLA sends DHCP Discover and Request packets, DHCP Option 12 now contains the WLA serial number, and DHCP Option 77 contains “WLA” (without the quotes).

By default, MSS has a database with 19 fingerprints that identify the following devices:
- iPhone
- iPad
- PC with Windows XP
- Android-based phones including Samsun, Motorola, HTC, LG, etc.
- OSX devices (Apple)
- WiFi-enabled game consoles such as PS3, Xbox, Wii for detection in school dorms.
- WinMobile and Nokia phones
- Kindle Fire
- Nook
- Printers

![Device Fingerprinting Diagram](image)  

Figure 3: An Example of Wireless Access based on Device Fingerprinting

Device fingerprints are processed in the configured order by MSS, and the MSS fingerprint database has the following characteristics:

- Maximum of 50 fingerprints supported
- Fingerprints must be uniquely named
- You can add, modify, or delete entries.

The following information is required by the device fingerprinting feature:

- Device type - used to identify the device.
- Rules - each rule defines these parameters:
  - Number - used to identify the rule
  - Type - the type of rule such as MAC address.
  - Data - contains the data from the packet.
• Value - the value to match against the data.
• Method - matching method used for the data and value.

The following rule types are supported:

• MAC Address
  • Data - the device MAC address
  • Value - MAC “glob” using the existing MAC rules in MSS
  • Method - MAC “glob” comparison

• DHCP Flags
  • Data - DHCP flags field
  • Value - 2 byte mask -
  • Method - Bitwise AND

• DHCP Option
  • Data - Byte data from the specified DHCP option.
    – Option number is an integer.
    – Option content is a string of consisting of either a string, hex, or an order sensitive list of
      DHCP option numbers.
    – Method - “eq” or “neq” based on the current MSS implementation. It matches if both are “eq”.
      “Contains” and “Not Contains” are also supported /

• DHCP Options List
  • Data - List of DHCP Options from the DHCP packet
  • Value - list of desired DHCP options in a format consistent with Options content list.
  • Method - one of “eq” or “neq” or “contains” or “not contain”

• Combination of rules - rules are not used directly in the detection process but combined to gether to
  create a rule expression. This consists of a logical expression specified as a string and can contain the
  following tokens:
  • rule number - one of the defined rules for this fingerprint
  • “and” and “or” used for logical tests
  • “(“and”)” used for grouping
  • white space - used for separation of the tokens.

Interactions between the User Policy and the Device Policy
Who wins? All attributes from a device policy and user policy are applied to a session except
when there are conflicts. When there is a conflict, device policies take precedence over user
policies by default. You can change the precedence in the CLI.

Other Functionalities Supported by Device Fingerprinting
Device detection works in parallel with AAA, so all AAA methods are compatible. It is also
supported in a cluster (high availability) environment.
Use Cases

- Controlling Network Access on a Corporate WLAN for a Personal iPad — A user joins the network through an 802.1X authentication process while using his personal iPad. Authentication is performed through a RADIUS server, credentials accepted, and an attribute is returned to the user allowing him to join VLAN1. The WLC detects that the user’s device is an iPad and applies a new ACL that only allows the user access to an e-mail server, and public internet access.

- Controlling User Bandwidth by Applying Different QoS Levels per Device Type — You want to apply a different CoS level when an authorized user authenticates onto the WLAN with an iPhone instead of a corporate device. A device-profile, iphone, is configured with an attribute that caps the bandwidth at 2 Mbps. When an iPhone user authenticates successfully using 802.1X and a RADIUS server, an attribute is sent that allows the user to access VLAN RED. The WLC detects that the user has an iPhone and applies the QoS profile restricting bandwidth to 2 Mbps.

Creating Device Fingerprints Using RingMaster

Informational Note:

RingMaster contains a number of preconfigured device fingerprints, but you must install MSS 8.0 on a WLC and upload the configuration into RingMaster. Otherwise, you must configure the device fingerprints individually. See the MSS Configuration Guide Version 8.0 for more information.
Device Fingerprinting is located under AAA in the WLC Configuration tree.

![Device Fingerprinting in RingMaster](image)

Figure 4: Device Fingerprinting in RingMaster

If you are going to use Device Profiles to apply QoS profiles or other attributes such as time-of-day, you should configure them before configuring your Device Fingerprint rules.

**Configuring Device Profiles**

Using RingMaster 8.0, select **Device Detection**, and then click **Create Device Profile**.
1. Enter a name for the Device Profile. In this example, you’ll create a Device Profile for mobile devices using iOS from Apple. Click Next.

2. If you select Deny All Matching Sessions, any device with this profile cannot connect to the WLAN. If you select additional attributes, such as time-of-day, then the mobile device cannot connect during the specified time period. In this example, you allow devices with iOS to access the network.

3. Select a VLAN for the mobile devices. You may want to put all of your mobile devices on one VLAN to segregate them from the rest of the wireless network.

4. You can apply the following attributes to the Device Profile:
   - **QoS Profile** - applies QoS policies to the devices.
   - **Filter id** - adds the portalacl.out to the profile. This will direct users to a Web portal for logging out of the network.
   - **Time of day** - configure specific times during the day that devices can access the network.
   - **Filter id** - applies the portal acl.in to direct users to a Web portal for logging onto the network.

5. Click Next to display the configured Device Fingerprints.

6. Select the fingerprint from the list of Available Device Fingerprints to apply the device profile, and move it to the Current Device Fingerprint list.

7. Click Finish to complete the configuration. You now have a Device Profile for mobile devices using iOS.

**Configuring Device Fingerprints Using RingMaster**

*Informational Note:* Default Device Fingerprints are available in RingMaster.

This section provides instructions on creating an iPhone Device Fingerprint as example of creating rules and using Boolean expression to create logical expressions.

You can now add device fingerprints to the RingMaster configuration. You may want to use the rule examples in the previous section to guide you through the rule configuration. Let’s add a Device Fingerprint for iPhones on your wireless network:
1. Click **Configure Device Fingerprint** to display the configuration wizard.

![Configure Device Fingerprint](image1.png)

2. In the **Device Type** field, type iPhone.
3. In the **Device Group** field, type iOS.
4. From the **Device Profile** list, select iOS, and click **Next**.

You need to create four rules that are used for DHCP device fingerprints as well as a logical rule expression for the device fingerprint.

![Create Device Fingerprint](image2.png)

5. Select **DHCP Option** to display the properties. Enter 12 as the **DHCP Option**, and then select contains as the operator. In the **Option value** field, enter iPhone.
6. Click **Ok**.
7. Select **DHCP Option List** and click Next.

8. Select the Option Number, the operand “is”, and then enter the content for the selected option. For this rule, the DHCP Options are 53, 55, 57, 61, 61, 51, 12.
Integrating a WLM1200-SP into RingMaster

With the release of RingMaster 7.5 and later, you can integrate your WLM1200-SP (SmartPass) server into RingMaster and use RingMaster to manage your WLM1200-SP server.

Informational Note:
You must have an active SmartPass server before you can integrate it into RingMaster. RingMaster communicates with the SmartPass server to synchronize the information in SmartPass with RingMaster. If the SmartPass server is inactive, then synchronization fails with RingMaster.

Caution:
To take advantage of the full functionality of SmartPass, install SmartPass Version 7.4.4.1 on your server. Earlier versions have less functionality than the latest version of SmartPass.

To integrate SmartPass into RingMaster, follow these steps:

1. In RingMaster, select your Network Plan.
2. From the Organizer panel, select Application Servers.
3. From the Tasks panel, select Create SmartPass Server.
4. To configure the SmartPass Server Connection Settings, you need the following information:
   - Server Name
   - IP Address
   - Port Number
   - Username
   - Password
5. Once you have entered the appropriate information, RingMaster sends a synchronization request to the SmartPass server.
6. The SmartPass server is now managed by RingMaster and displayed in the list of SmartPass Servers.
7. To configure the server settings, select it from the list and click Properties.
8. Adjust the necessary settings and click Ok to save the configuration.
9. After adding the SmartPass Server, and you synchronize the server with RingMaster successfully, additional tasks are now available in RingMaster. These are the same tasks available in a standalone installation of SmartPass. You can refer to the SmartPass documentation for more information on configuring these features. The following tasks are now available:
   - Setup
– Synchronize
– Edit SmartPass Server
– Shared Key

Other
– Server Settings
– RADIUS Client Settings
– Web Portal Management
– User Management
– User Type Management

Clicking on any of the tasks under Other opens the current installation of SmartPass.
Integrating a WMS1200-LA to RingMaster

To add a WMS1200-LA to RingMaster, you must install a WMS1200-LA in your wiring closet or located somewhere in your network. After installation, you need the following information to add the WMS1200-LA to RingMaster:

- IP Address
- User Name
- Password

You also need a Location Appliance license in order to activate the feature in RingMaster. After installing the license, the Create Location Server task is available in the RingMaster interface.

To add a WMS1200-LA to RingMaster, follow these steps:

1. Open RingMaster and click Configuration from the menu bar.
2. From the Organizer panel, select Application Servers.
3. From the Task list, select Create Location Server and the associated wizard opens.
4. Select Managed to allow RingMaster to manage the location appliance.
5. In the Name field, enter the name of the WMS1200-LA.
6. Enter the IP address.
7. Enter the User Name.
8. Enter the Password.
9. If there is a management password, enter the password in the Management Password field.
10. Click Next. RingMaster connects to the WMS1200-LA and establishes a connection.
11. Click Finish to complete the configuration.
12. The WMS1200-LA now appears in the Organizer panel under Application Servers.

To review WMS1200-LA settings, highlight the Location Appliance in the list and click Properties. You can then change any of the original settings for the server.

Available Tasks for All Managed WMS1200-LA Location Appliances

There is a list of available tasks for all location appliances managed by RingMaster. You can select any of the following tasks:

- Create Location Server
- Setup Synchronization Parameters
- Edit a Location Server
- Configure a Snoop Filter
- Configure SNMP Settings

From the Other List, you can select from the following tasks:

- Platform Management
- Appliance Logs
- Backup and Restore
• Configuration
• Factory Reset
• Schedule Reboot
• System Update
• User Management

Selecting any of the Other tasks opens the corresponding software feature on the location appliance. For more information on using these features, refer to the Juniper Networks WMS1200-LA User’s Guide.

Available Location Appliance Tasks

If the location appliance already has a configuration, the details are displayed when you select the WMS1200-LA in the Organizer panel.

After it is selected, the following information is displayed:

• Location Server
• Managed
• Name
• Port
• Version
• IP Address
• Locales
• Name
• Description
• Associated Fingerprints
• Associated Floor
• RF Fingerprints
• Name
• Description
• Associated Locale

In the Tasks panel, you can select from a list of available tasks. Under Create, you can select

• Create Locale
• Create RF Fingerprint
• Under Setup, you can select
• Synchronize
• Edit Location Server
• Snoop Filter
• SNMP
• Under Other, you can select
Selecting any tasks under Other, opens the operating system of the location appliance and you can perform any of these tasks directly on the location appliance.

Creating Locales Using RingMaster
Select an WMS1200-LA from the Application Servers list in the Organizer panel. The Task list is now populated with available tasks to perform on the location appliance. To create a locale, use the following steps:

1. Under Create, click Create Locale. The Create Locale Wizard is displayed.
2. Enter the name and description of the locale in the appropriate fields. Create RF Fingerprint is selected by default. If you do not want to create an RF Fingerprint, clear the checkbox. If you are also using Active Asset on the location appliance, you must follow a specific format for the description. The format is Campus:Building:Floor. Click Next.
3. Enter the RF Fingerprint information including Name and Description. Click Next.
4. If there are other RF Fingerprints configured on the location appliance, they are displayed in the Available RF Fingerprints list. You can select one and add it to the Current RF Fingerprints list. You can also remove RF Fingerprints by selecting one from the Current RF Fingerprints list and clicking Remove.
5. Click Finish to complete the configuration. The new locale and RF Fingerprints appear in the Location Server and RF Fingerprints section. You can view the properties of a RF Fingerprints by selecting it and then clicking Properties.

Creating Locales Using RF Planning
You can also create Locales using the RF Planning feature of RingMaster. Click RF Planning and select a plan from the Organizer. You can also import locales from CAD drawings.

1. Under Location Services, click Create Locale. The Create Locale wizard is displayed.
2. When you use the Drawing tools to draw the Locale, the Create a Locale wizard is displayed.
3. Select a Location Server from the list and click Next.
4. You can now select an existing locale or create a new locale. If you select an existing locale, click Finish to complete the configuration. If you select Create a Locale, click Next.
5. Type a name and description of the Locale in the Name and Description fields. Click Finish to complete the configuration.
Adding RF Fingerprints Using RF Planning

You can add RF Fingerprints to the Locale you just created by clicking RF Fingerprint in the Task list. When you move your cursor over the locale, it changes to a crosshair. Click and drag to display the RF Fingerprint wizard.

Enter a name and description for the RF Fingerprint and click OK. The RF Fingerprint now appears on the Locale.

Calibrating RF Fingerprints Using RF Planning

1. To calibrate an RF Fingerprint, click on the fingerprint icon in the locale to select it. Then click Calibrate RF Fingerprint.

2. Enter the MAC address of the device and click Start. You can see the status in the Progress bar. Once the process is complete, you can click Next to add it to the locale.

3. Creating RF Fingerprints

4. Select an WMS1200-LA from the Application Servers list in the Organizer panel. The Task list is now populated with available tasks to perform on the location appliance. To create a RF Fingerprint, use the following steps:

5. Under Create, click Create RF Fingerprint. The wizard is displayed.

6. Enter a name and description for the RF Fingerprint.

7. Click Next.

8. Select a locale from the Associated Locale list to associate with the RF Fingerprint.

9. Click Finish to complete the configuration.

10. The RF Fingerprint now appears in the Locales list and the RF Fingerprints list.

11. Setting Up a Location Appliance Using RingMaster

12. Select an WMS1200-LA from the Application Servers list in the Organizer panel. The Task list is now populated with available tasks to perform on the location appliance.

13. Synchronizing Changes on a Location Appliance using RingMaster

14. To synchronize configurations on a location appliance, use the following steps:

15. In the Task list, click Synchronize.

16. The Review Changes panel is displayed.

17. You can select from two types of action:

18. Deploy Changes to the location appliance - changes made using RingMaster are applied to the location appliance.

19. Accept Changes from the location appliance - changes made on the location appliance are uploaded to RingMaster.

20. You cannot undo this operation. Once you click Next, the changes are synchronized between RingMaster and the LA-200.

21.
23. Click Next. The changes are synchronized between RingMaster and the location appliance.
24. Click Finish to complete the operation.

The WMS1200-LA image created using RingMaster is transferred to the WMS1200-LA where it is used by other applications such as Active Asset. It is recommended that you create a backup of your current image before transferring the new one to the WMS1200-LA.

**Editing Location Appliance Attributes Using RingMaster**

To edit a location appliance, select it from the list of Application Servers. Then follow these steps:

1. Click Edit Location Server to display the attributes for the server.
2. You can modify any of the listed attributes, and click Next.
3. RingMaster establishes a connection with the location appliance. Click Finish to send the changes to the location appliance.

**Configuring a Snoop Filter for a Location Appliance**

5. You can configure a snoop filter on a WLC using RingMaster and apply it to a location appliance. To configure a snoop filter, follow these steps:

6. In the Task list, under Setup, click Snoop Filter.
7. Select an WLC to target from the Select a WLC list.
8. Click Next.
9. If there is an existing Snoop Filter on the WLC, you can select it from the Filters list. If a Snoop Filter is not configured, you can select Create a Filter. Click Next. Enter the Snoop Filter Name field, enter a name for the filter. Select Enabled to begin using the filter. Click Next.
10. Configure the Snoop Filter Observer. You must specify the following information:
   - Target IP Address
   - Snap Length Limit (optional)
   - Frame Gap Limit (optional)
11. Click Next.
12. Optionally, you can create Snoop Filter Conditions by specifying a list of conditions that match the criteria for packets. The following conditions can be added to the Snoop Filter:
   - Direction
   - Frame Type
   - Channel
   - BSSID
   - Source MAC
   - Destination MAC
   - Host MAC
   - MAC Pair
13. When you select a condition, a list of attributes is displayed that can be applied to it. Click Next.

14. You can also configure optional Snoop Mapping by selecting radios on an MP to map the Snoop Filter. Click Next.

15. Additionally, you can map a Snoop Filter to a specific radio profile. Select one from the Available Radio Profiles list and click Add to move it into the Current Radio Profiles list.

16. Click Finish to complete the Snoop Filter configuration.

Configuring SNMP for a Location Appliance

You can configure SNMP settings for the Location Appliance using the RingMaster interface. Select a Location Appliance from the list in the Organizer panel and then click SNMP.

You need the following information to configure SNMP targets on the Location Appliance:

- Destination Host
- Destination Port
- SNMP Version

If you select SNMP Version v2c, then you configure the SNMPv2c Settings. If you select SNMPv3, then you configure the SNMPV3 settings. Click Next to continue with the configuration.

If you a secondary SNMP target, you can configure it by entering the appropriate information. Click Finish to complete the configuration.

All tasks listed under Other are performed on the WMS1200-LA using the WMS1200-LA user interface. Consult the documentation for the WMS1200-LA to perform any of these tasks. Coverage of these tasks is beyond the scope of this document.

Monitoring the WMS1200-LA

You can see the following status information on the WMS1200-LA when you click Monitoring and then select the WMS1200-LA from the Organizer panel.

The Monitor feature displays the following information:

- Status Summary — click Details for more information.
- Appliance Name
- Status
- Admin Status
- IP Address
- Server Type
- Management Port
- Version
- Up Time
- Alarm Summary — click Details for more information.
• Clients by Locale — you can also click Find Clients to search for clients on the network.
• Tracked Devices by Type

Additional WMS1200-LA Areas Monitored by RingMaster

There are additional features on the WMS1200-LA that can be monitored by RingMaster. When you select a floor with a WMS1200-LA, a new Show Devices task is available. This task displays all the devices tracked by the WMS1200-LA including:
  • Clients
  • Tags
  • APs
  • Rogue APs

You can filter the devices displayed using the following strings:
  • SSID
  • User Name
  • MAC Address
  • IP Address
  • End Address for SIP
  • Radio Technology

When you use the filtering capabilities, only the devices matching the filter are displayed. Once you clear the criteria, all devices are displayed again.

You can also hide or display the following items on the Monitoring interface:
  • Locales
  • Fingerprints
  • APs
  • Clients (Voice and Data)
  • Tags
  • Rogue APs
  • Client and AP Connections

When you select Show Devices and then select an asset tag, you can see the temperature of the tag as well as the battery life for the tag.

Configuring NAS-ID for an MP Using the CLI

To set the NAS-ID of an MP, use the following command:

```
WLC# set ap apnum ap-nas-id string
```

The maximum length of the string value is 24 hexadecimal characters.

To set the URL format, use the following command:

```
WLC# set service-profile profilename web-redirect-url-format [standard | cmcc]
```

To set the NAS-ID for the WLC as a RADIUS attribute, use the following command:

```
WLC# set radius nas-id string
```
The maximum length of the string value is 24 hexadecimal characters.

To display the status of external sessions, use the following command:

```
WLC# show sessions external-web-auth [client-ip ipaddr] verbose
```

```
Client         Portal       SessionID        User Name     State
-------------------------------
192.168.111.21 192.168.10.10   4             user-1        Exchange
```

If verbose is specified, the output is displayed as follows:

```
Client IP:          192.168.111.21
Username:           user-1
Portal:             192.168.10.10
Portal Port:        12345
Portal Serial:      0xabcd
Session ID:         10
State:              Accounting
Last Error code:    0
```

For RingMaster, the configuration is located under Access Points.

**WMS1200-LA Alarms Displayed by RingMaster**

The following WMS1200-LA alarms are displayed in the Alarms panel of RingMaster:

- AP Snoop Status
- Agent Status
- Asset Tag Button Pressed
- Asset Tag Battery Low
- Asset Tag Detached
Integrating an AirTight Server into RingMaster

Overview
SpectraGuard Enterprise is a complete, end-to-end wireless intrusion prevention solution (WIPS) used by some of the world’s largest enterprise firms. You can now add AirTight servers to your RingMaster configuration. AirTight is a wireless security system that can track unwanted access or attempts to access your wireless network. For more information on AirTight, see the Web site at http://www.airtightnetworks.com.

Adding the AirTight Server to RingMaster
1. After you log into RingMaster, click Configuration. In the Organizer panel, select Application Servers.
2. The options for Application Server are displayed in the Tasks panel. Click Create AirTight SGD Server to launch the configuration wizard.
3. Enter the configuration information into the following fields:
   - Name — The name of the AirTight server
   - IP Address — Enter the IP Address of the AirTight server.
   - Username — The username required to authenticate on the server.
   - Password — The password required to complete the authentication process on the server.
4. If you are not enabling SNMP for the AirTight server, clear Enable Traps. It is selected by default.
5. Click Next.
6. RingMaster now attempts to connect to the AirTight SGE server and synchronize with it.
7. After RingMaster synchronizes with the AirTight server, click Next to continue the integration.
8. You can now configure SNMP on RingMaster to process traps from the AirTight SGE Server. Select the SNMP version from the list and then configure the v2c settings.

Informational Note:
Because AirTight uses a proprietary configuration for SNMP, you cannot configure SNMP Version 3 as the SNMP setting.

9. Click Next to complete the configuration. The AirTight Server is now displayed in the Security Servers section of the Application Servers page.
10. To edit the AirTight Server properties, select the AirTight SGE Server and click Properties. You can edit the same information that you configured using the wizard.

Informational Note:
Before you can integrate an AirTight Server, you must purchase and install the RingMaster license, RMTS-SECURITY-ADV.
For specific information about AirTight SGE Server and its configuration, please consult the AirTight SGE Server documentation.

Adding Alarms for the AirTight Application Server

You can configure RingMaster to display alarms for the AirTight application server. To add or remove alarm categories, follow these steps:

1. Click **Alarms**, and then **Setup**.
2. Click the AirTight SGE Settings tab.
3. All AirTight alarms are enabled by default. Clear checkboxes next to the alarms that you do not want monitored.
4. Click **Close** to save your alarm settings.
5. You can also query the **Alarms** database for AirTight-specific alarms. Click **Query**, and then select Security Server from the Type list.
6. From the **Instance** list, select Application Servers: AirTight.
7. Select the date and time range for the query.
8. Then select the **Categories**, **Severities**, and the **States**.
9. Click **OK** to execute the query against the **Alarm** database.

Creating AirTight Reports Using RingMaster

You can create AirTight reports by clicking on Reports in the RingMaster interface, and then clicking Report under Generate in the Task list.

1. From the **Organizer** list, select **Alarms** and then **Alarm Summary**.
2. From the **Task** list, under **Generate**, click **Report**.
3. From the **Report Scope Type** list, select **Security Server**.
4. Click **Next**.
5. Select the type of format for the report from the Report Format list. Also, specify an e-mail address if you want the report sent via e-mail. Then specify if you want the report sent as a hyperlink in the e-mail or attached as a PDF.
   
   You can also copy the report to an FTP server. You must configure the FTP server as part of the overall Report Settings located under Setup in the Tasks list.
6. When you click **Next**, a link is generated to the report.
7. When you click on the link, the **Alarm Summary Report** is displayed in your Web browser.
Policies Overview

A policy is a set of WLC configuration parameters defined in RingMaster and then applied to multiple WLCs. When you apply a policy to a set of WLCs, all parameter settings in the policy are applied to the WLCs and update previous settings on these WLCs.

Managing Changes

When you create a new policy, none of the settings for the policy are applied to WLC switches (even the ones you associate with the policy when you create it), until you explicitly apply the policy to the switches.

After associating a new policy with a switch, all new switches that match the WLA model and version number of the policy automatically receive the parameter settings in the policy. New switches are switches created using the WLC Switch wizard or any uploaded switches. However, policy changes are not automatically applied to switches. Reapply the changed policy to associated switches after making any changes to the policy.

Example of a Policy for a Large Network Deployment

In some cases, large network deployments consist of multiple instances of the same WLC models. A policy can be created in RingMaster and applied to the same modes without configuring the individual controllers.

For example, you may want to apply the same AAA parameters or wireless profile parameters to all WLC800s in your network. By creating a policy that is applied to all WLC800s, the policy is automatically applied by default when new WLC800s are added to the network.
Policy Example for Provisioning WLCs based on Roles

As you expand your network, you may have some criteria for your network that includes smaller controllers in the branch and larger ones in the data center. These controllers may offer different services based on a role they have in the network. Applying these configurations on multiple controllers, based on model filtering, is easily performed at the policy application phase.

For example, you could have remote WLAs connected to WLC2s which require remote WLA features based on a location or a policy such as guest access.
Policies Overview

Create Policy

Policy Setup

Enter a unique name for the Policy. You can optionally specify a WLC type and a version filter.

Policy Name: ProvisionAP
WLC Model Filter: WLC2
WLC Version Filter: 7.5.x

Create Policy

Policy Areas

Select all of the configuration areas that will be part of this policy.

System

- Management Services
- IP Services
- AAA, Spanning Trees and VLAN 802.1Q Restrictions
- Port Groups
- ACLs
- GoS Profiles
- LDP

Wireless

- Auto XGA
- Local Switching
- RF Detection
- Wireless Services and Radio Profiles
- Mobile Releasing
- RF Snop and Sweep Observer Table

AAA

- RADIUS
- Local User Database
- Location Policy
- 802.1X
- Admin and Network Access Rules and AAA Profiles
- Mobility Profiles
Configuring Policies

When you create a new policy, policy settings are not applied to WLCs (even the ones you associate with the policy when you create it), until you explicitly apply the policy to the WLCs. After associating a new policy with a WLC, all new WLCs matching this WLC model and version number of the policy automatically receive the parameter settings in the policy. New WLCs are WLCs created using the Create WLC wizard or any uploaded WLCs. However, policy changes are not automatically applied to WLCs. You must re-apply changed policies to associated WLCs after making any changes to a policy.

Use the following steps to create Policies:

1. Access the **Create Policy** wizard.
   a. Select the **Policies Navigation Bar** button.
   b. In the **Tasks** panel, select **Create Policy**.

2. In the **Policy Name** field, type a name for the policy. This name appears in the **Organizer** panel when the **Policies Navigation Bar** button is selected.

3. To configure a policy for a specific WLC model, select a model from the **WLC Model Filter** list.

4. To configure the policy to support an older version of RingMaster, select the version from the **WLC Version Filter** list.

5. Click **Next**.

6. Make policy creation option selections, including:
   a. **Create a new Policy** — Create a new policy with the name entered.
   b. **Create a Policy from a Device** — Create a new policy from that of a selected device.
   c. **Create a Policy from another Policy** — Create a new policy from another existing Policy.

7. Click **Next**.

8. Select the feature areas you want to set in a policy. When you apply a policy to an WLC, all parameter settings from selected feature areas are applied to the WLC. This includes default settings in the policy.

9. Click **Next**.

10. From **Available Devices** list, select WLCs to apply a policy, then click **Add** to move these WLCs to the **Current Devices** list.

11. Click **Finish**.

---

**Informational Note:**

Moving a WLC to the Current Devices list does not automatically apply the policy to the WLC. To apply policy settings, see Applying Policy Changes to WLCs.
Applying Policies

1. Select **Apply** in the **Tasks** panel to apply the changes to WLCs associated with a policy.
2. Review the list of WLCs, then click **Apply**. These changes are automatically applied to WLCs associated with the policy.
3. After the task is complete, click **Close**.
4. Repeat step 2 through step 3 for each policy category.
Verifying Configuration Changes

RingMaster employs a set of rules to verify WLC configurations. Changes to an WLC configuration in RingMaster or in a network are evaluated by comparing changes to rules. If this evaluation detects error or warning conditions, the Alerts panel is updated:

- Errors or warnings on a WLC configuration in RingMaster affect Configuration counts.
- Errors or warnings on the network affect Alarm counts.

Viewing the Verification Panel

Click on the word Config: (error list) in the Alerts panel to display the Verification panel, which shows errors and warnings for WLC configuration information in RingMaster. The upper section lists error descriptions in red and warning descriptions in orange:

- Errors are serious problems that must be addressed before deployment. By default, you cannot deploy a network plan with errors in it. After correcting errors, verify the network plan again to verify errors have been resolved.
- Warnings are non-critical issues that do not prevent deployment. Review any warnings and consider resolving the issues before deployment.

Details about selected errors or warnings appear in the lower left section of the panel. The Resolution section lists options for resolving a warning or error.

Filtering the Message List

By default, all warning and error messages are listed. You can click on the Filter checkbox to filter a message list. You can use the State menu to make selections. Menu choices are as follows:

- (All) — All messages are listed when this option is selected.
- Error — Only Error messages are listed when this option is selected.
- Error (Disabled) — Only Disabled rules are listed when this option is selected.
- Warning — Display only Warning messages when this option is selected.

Resolving a Warning or Error Message

For most errors and warnings, RingMaster provides a link to the configuration information that caused the error or warning. The link appears in the Resolutions section of the panel, under the Messages column. When you click the Edit link, RingMaster opens a configuration wizard for the configuration item. For example, if you create a new WLC called user-WLCr2 but you do not specify the system IP address of the WLC, the error message System IP address is not assigned or is invalid appears in the Message area. To correct the error, click on Edit user-WLCr2 in the Resolutions section. The Modify WLC wizard appears. Use the wizard to edit the System IP address. After saving this configuration change, RingMaster re-evaluates the configuration. If the system IP address is specified, the error no longer appears in the Verification panel.

To resolve an error or warning:

1. Select the error or warning message in the Message column.
2. Read the information in the Details area. For some errors and warnings, this section contains information about how to resolve the error or warning.

3. If a hint is listed in the Resolutions section, click on the option to display the configuration wizard for that item.

4. Edit the configuration item or resolve the network issue and save the change.

5. Refresh the information in the Verification panel.

6. Verify that the message no longer appears in the Verification panel.

**Disabling a Rule in the Message List**

All RingMaster rules are enabled by default. If you want RingMaster to stop alerting you about a specific error or warning, you can disable the rule for that error or warning. You can disable rules on a per-instance basis or globally for all instances.

- If you disable a rule for a specific instance, RingMaster stops alerting you about that particular instance but still uses the rule when evaluating other configuration items.
- If you disable a rule for all instances, RingMaster stops using that rule altogether when verifying a configuration.

---

**Informational Note:**

Rules that are disabled for all instances are disabled on a per-user basis, not a per-plan basis. When you disable all instances of a rule, the rule is disabled for any network plan that you open while logged on with the RingMaster Client user name used when you disabled the rule.

---

To disable a specific instance of a warning or error:

1. Select a warning or error message.

2. In the Resolutions section, click Disable this rule for this instance only. When you enable this option, the message disappears from the list. RingMaster does not display this particular instance of the message again.

To globally disable a warning or error:

1. Select an instance of the warning or error message.

2. In the Resolutions section, click Disable this rule for all instances. When you enable this option, all instances of the message disappear from the list. RingMaster does not display the message again.

**Changing Verification Options**

By default, RingMaster verifies configuration information in the following cases:

- Configuration is changed in RingMaster.
- Deploy or export a WLC from RingMaster to the network.
- Upload a WLC from the network into RingMaster.

RingMaster verifies an WLC configuration by default each time a change occurs. In addition, it allows you to deploy or export configuration changes that cause error messages by default.
To change verification options:

1. In the Tasks panel, while viewing the Verification panel, click Edit Verification Options and the multi-tabbed Verification Options dialog box is displayed. The first tab shown is the Options tab:

2. Select the cases for RingMaster to perform verification:
   
   - Verify changes only — RingMaster performs verification only on configuration items that change, rather than the entire configuration when any change in that configuration occurs.
   
   - Verify on edits — RingMaster performs verification whenever you edit a configuration.
   
   - Verify on deploy and export — RingMaster performs verification when you select the option to deploy WLCs from RingMaster to the live network.
   
   - Verify on upload — RingMaster performs verification when you select the option to upload a configuration from the network into RingMaster.
   
   - Allow errors to be deployed and exported — RingMaster allows you to deploy or export a configuration even if it contains errors.

3. Click Close to place the changes into effect and close the dialog box.
Adding a Third Party AP to a Network Plan

You can add a third-party AP to an equipment list of a network plan. When you use RF Planning, you can place an AP at its location on a floor plan. In this case, RingMaster takes the channel number of the AP into account when assigning channels to APs.

To add a Third Party AP:

1. Select the Configuration Navigation Bar button.
2. Select the network plan in the Organizer panel.
4. In the Name field, type a name for the access point. You can use 1 to 32 characters, with no punctuation except the following: period (.), hyphen (-), or underscore (_).
5. Optionally, in the Manufacturer ID field, type the manufacturer identification for the access point (1 to 30 characters, with no spaces).
6. In the Product ID field, type the product identification for the access point (1 to 30 characters, with no spaces).
7. In the IP Address dialog, type the IP address for the access point.
8. If you specify an IP address, you can use Telnet and a Web browser with this access point.
9. In the Telnet Port Number field, specify the port number for Telnet service.
10. In the HTTP Port Number field, specify the port number for HTTP service.
11. Click Next.
12. From the AP Model list, select one of the following:
   - AP (Dual Radio) — 802.11a and 802.11b or 802.11b/g
   - AP (Single Radio) — 802.11a, 802.11b, or 802.11g
13. In the Radio Type list, select one of the following: 11a, 11b, 11g. The choices available depend on the selection you made in step 11.
14. Click Next.
15. Verify the radio slot number and radio type. For a dual-radio access point, 802.11b/g radios have a slot number of 1. 802.11a radios have a slot number of 2.
16. From the Channel Number list, select the channel number for the radio.
17. In the Transmit Power field, specify the transmit power for the radio.
18. To enable the radio, select Enabled.

**NOTE:** The radio for the access point must be enabled to be considered in channel allocation.

19. In the SSID field, type the Service Set Identifier (SSID) for the radio.
20. In the MAC Address field, type the MAC address of the radio.
21. From the Antenna Gain list, select the antenna gain for the radio.
22. If the access point has only one radio, click Finish. Otherwise, go to step 22.
23. Click Next. The Radio A page appears.
24. Repeat step 14 through step 20 for the 802.11a radio.
25. Click Finish to save changes.