Configure Wireless Devices

View All Controllers in Cisco Prime Infrastructure

You can view a summary of all controllers in the Prime Infrastructure database.

Note If you enable wireless on Cisco Catalyst 9500, 9400, or 9300 Switches, Cisco Prime Infrastructure lists them as switches and not as WLAN controllers.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 To use the command buttons at the top of the page, select the check box next to one or more controllers. The following table describes the field available in this page.

Table 1: Wireless Controller Summary Information

Field	Description
Admin Status	Administration status of the wireless controller.
DNS Name	DNS name of the wireless controller.
Last Inventory Collection Status	Status of the last inventory collection.
Last Successful Collection Time	Last successful collection time.
Client Count	Displays the total number of clients currently associated with the controller
Software Type	Displays the software type of all managed devices.
Location	Displays the location information .
Device Name	Name of the controller. Click on a device name to view device details, configure the controller, apply templates, view and schedule configuration archives, and view and update the controller software image.
Reachability	Reachability status is updated based on the last execution information of the Device Status background task.
IP Address/DNS	Local network IP address of the controller management interface. Click the icon under the IP address to launch the controller web user interface in a new browser window.

Field	Description
Device Type	Based on the series, device types are grouped. For example: • WLC2100—21xx Series Wireless LAN Controllers • 2500—25xx Series Wireless LAN Controllers • 4400—44xx Series Wireless LAN Controllers • 5500—55xx Series Wireless LAN Controllers • 7500—75xx Series Wireless LAN Controllers • WiSM—WiSM (slot number, port number) • WiSM2—WiSM2 (slot number, port number)
AP Discovery Status	Indicates whether the AP discovery has completed.
Software Version	The operating system release. version. dot. maintenance number of the code currently running on the controller.
Mobility Group Name	Name of the mobility or WPS group.

Step 3 To view specific information about a controller, click on a Device Name.

Related Topics

Controller-Specific Commands for Configuration Template Deployments, on page 4

Controller-Specific Commands for Configuration Template Deployments

When you choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller and select the checkbox next to one or more devices, the following buttons appear at the top of the page:

- Delete—Allows you to delete a controller.
- Edit—Allows you to edit general parameters, SNMP parameters, Telnet/SSH parameters, HTTP parameters, and IPSec parameters.
- Sync—
- Groups & Sites—Allows you to add and remove controllers from location groups and sites.
- Reboot—Enables you to confirm the restart of your controller after saving configuration changes. You can select these reboot options:
  - Save Config to Flash—Data is saved to the controller in non-volatile RAM (NVRAM) and is preserved in the event of a power cycle. If the controller is rebooted, all applied changes are lost unless the configuration has been saved.
  - Reboot APs
  - Swap AP Image
- Download—Allows you to select the following options to download software to controllers.
  - Download Software—Choose from TFTP, FTP, SFTP to download software to the selected controller or all controllers in the selected groups after you have a configuration group established.

- Download IDS Signatures
- Download Customized Web Auth
- Download Vendor Device Certificate
- Download Vendor CA Certificate
- Bulk Update Controllers

- Configure
  - Save Config to Flash
  - Discover Templates from Controller
  - emplates Applied to Controller
  - Audit Now
  - Update Credentials

Related Topics

View All Controllers in Cisco Prime Infrastructure, on page 3
Check Which Configuration Templates Are Used by Controllers and Remove the Associations, on page 5
Change Controller Credentials Using an Imported CSV File, on page 7
Apply Controller Changes By Rebooting, on page 7
Download Software to Controllers, on page 8

Check Which Configuration Templates Are Used by Controllers and Remove the Associations

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type > Wireless Controller**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click **Configure > Audit Now**.

Step 4 Click **OK** in the pop-up dialog box to remove the template associations from configuration objects in the database as well as template associations for this controller from associated configuration groups (This is a template-based audit only).

You can specify for which Prime Infrastructure configurations you want to have associated templates.

The templates that are discovered do not retrieve management, local, or guest user passwords.

The following rules apply for template discovery:

- Template Discovery discovers templates that are not found in Prime Infrastructure.
- Existing templates are not discovered.
- Template Discovery does not retrieve dynamic interface configurations for a controller. You must create a new template to apply the dynamic interface configurations on a controller.

Related Topics

View Controller Audit Results in a Report, on page 6
View Templates That Have Been Applied to Controllers, on page 18

Discover Existing Templates for Controllers, on page 18
Apply Controller Changes By Rebooting, on page 7
Download Software to Controllers, on page 8
Replacing Controllers While Retaining the IP Address, on page 19

Change Controller Credentials from the Network Devices Table

To update SNMP and Telnet credentials, you must do so on each controller. You cannot update SNMP/Telnet credential details for multiple controllers at the same time.

SNMP write access parameters are needed for modifying controller configuration. With read-only access parameters, configuration can be displayed only and not modified.

To update the SNMP/Telnet credentials, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type** > **Wireless Controller**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click **Configure > Update Credentials**.

Step 4 Complete the required fields, then click **OK**.

Related Topics

Change Controller Credentials Using an Imported CSV File, on page 7

View Controller Audit Results in a Report

After you perform an audit on a controller, the Audit Report displays the following information:

- Device Name
- Time of Audit
- Audit Status
- Applied and Config Group Template Discrepancies information including the following:
  - Template type (template name)
  - Template application method
  - Audit status (For example, mismatch, identical)
  - Template attribute
  - Value in Cisco Prime Infrastructure
  - Value in Controller
  - Other Cisco Prime Infrastructure Discrepancies including the following:
  - Configuration type (name)
  - Audit Status (For example, mismatch, identical)
  - Attribute

- Value in Controller
- Total enforcements for configuration groups with background audit enabled. If discrepancies are found during the audit in regards to the configuration groups enabled for background audit, and if the enforcement is enabled, this section lists the enforcements made during the controller audit. If the total enforcement count is greater than zero, this number appears as a link. Click the link to view a list of the enforcements made from Cisco Prime Infrastructure.

- Failed Enforcements for Configuration Groups with background audit enabled—If the failed enforcement count is greater than zero, this number appears as a link. Click the link to view a list of failure details (including the reason for the failure) returned by the device.
- Restore Cisco Prime Infrastructure Values to Controller or Refresh Configuration from Controller—If there are configuration differences found as a result of the audit, you can either click **Restore Prime Infrastructure Values to controller** or **Refresh Config from controller** to bring Cisco Prime Infrastructure configuration in sync with the controller.
  - Choose **Restore Prime Infrastructure Values to Controller** to push the discrepancies to the device.

Related Topics

Check Which Configuration Templates Are Used by Controllers and Remove the Associations, on page 5

Change Controller Credentials Using an Imported CSV File

You can update multiple controllers credentials by importing a CSV file.

To update controller(s) information in bulk, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices**, select **Wireless Controllers**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click **Download > Bulk Update Controllers**.

Step 4 Enter the CSV filename in the Select CSV File text box or click **Browse** to locate the desired file.

Step 5 Click **Update and Sync**.

Related Topics

Change Controller Credentials from the Network Devices Table, on page 6
Apply Controller Changes By Rebooting, on page 7
Replacing Controllers While Retaining the IP Address, on page 19

Apply Controller Changes By Rebooting

You should save the current controller configuration prior to rebooting. To reboot a controller, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, select **Wireless Controllers**, then click **Reboot > Reboot Controllers**.

Step 2 Select the required Reboot Controller option:

- Save Config to Flash—Data is saved to the controller in non-volatile RAM (NVRAM) and is preserved in the event of a power cycle. If the controller is rebooted, all applied changes are lost unless the configuration has been saved.
- Reboot APs—Select the check box to enable a reboot of the access point after making any other updates.
- Swap AP Image—Indicates whether or not to reboot controllers and APs by swapping AP images. This could be either Yes or No.

Step 3 Click **OK**.

Related Topics

Change Controller Credentials from the Network Devices Table, on page 6
Replacing Controllers While Retaining the IP Address, on page 19

Download Software to Controllers

To download software to a controller, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type > Wireless Controllers**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click **Download** and select one of the following options:

- **Download Software TFTP**
- **Download Software FTP**
- **Download Software SFTP**

Step 4 Complete the required fields.

Step 5 Select the download type. The pre-download option is displayed only when all selected controllers are using Release 7.0.x.x or later.

- Now—Executes the download software operation immediately. If you select this option, proceed with Step 7.
- Scheduled—Specify the scheduled download options.
  - Schedule download to controller—Select this check box to schedule download software to controller.
  - Pre-download software to APs—Select this check box to schedule the pre-download software to APs. The APs download the image and then reboot when the controller reboots. To see Image Predownload status per AP, enable the task in the **Administration** > **Dashboards** > **Job Dashboard** > **System Jobs** > **Wireless Poller** > **AP Image Pre-Download Status**, and run an AP Image Predownload report from the Report Launch Pad.
  - FlexConnect AP Upgrade—Select this option to enable one access point of each model in the local network to download the image. The remaining access points will then download the image from the primary access point using the pre-image download feature over the local network, which reduces the WAN latency.

Step 6 Select the Schedule options.

Schedule enough time (at least 30 minutes) between Download and Reboot so that all APs can complete the software pre-download. If any AP is in pre-download progress state at the time of the scheduled reboot, the controller will not reboot. You must wait for the pre-download to finish for all the APs, and then reboot the controller manually.

Step 7 Enter the FTP credentials including username, password, and port.

You can use special characters such as @, #, ^, *, ~, _, -, +, =, {, }, [,], :, ., and / in the password. You cannot use special characters such as $, ', \, %, &, (,), ;, ", <, >, , , ? , and | as part of the FTP password. The special character "!" (exclamation mark) works when the password policy is disabled.

Step 8 Select whether the file is located on the **Local machine** or an **FTP Server**. If you select FTP Server, the software files are uploaded to the FTP directory specified during the installation.

Step 9 Click **Download**.

If the transfer times out, choose the FTP server option in the **File is located on** field; the server filename is populated and Cisco Prime Infrastructure retries the operation.

Upload Controller Configuration and Log Files to an FTP/TFTP Server

You can upload a controller system configuration to the specified TFP or TFTP server as a file. Both File FTP and TFTP are supported for uploading and downloading files to and from Prime Infrastructure. To upload files from a controller, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click a Device Name, then click the **Configuration** tab.

Step 3 From the left sidebar menu, choose **System** > **Commands**.

Step 4 Select the **FTP** or **TFTP** radio button, then select **Upload File from Controller** and click **Go**.

Step 5 Complete the required fields.

Prime Infrastructure uses an integral TFTP and FTP server. This means that third-party TFTP and FTP servers cannot run on the same workstation as Prime Infrastructure because Prime Infrastructure and the third-party servers use the same communication port.

Step 6 Click **OK**. The selected file is uploaded to your TFTP or FTP server and named what you entered in the File Name text box.

Download IDS Signatures to Controllers

Prime Infrastructure can download Intrusion Detection System (IDS) signature files to a controller. If you specify to download the IDS signature file from a local machine, Prime Infrastructure initiates a two-step operation:

1. The local file is copied from the administrator workstation to Prime Infrastructure built-in TFTP server.
2. The controller retrieves that file.

If the IDS signature file is already in the Prime Infrastructure server's TFTP directory, the downloaded web page automatically populates the filename.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type** > **Wireless Controller**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click **Download** > **Download IDS Signatures**.

Step 4 Complete the required fields.

Step 5 Click **Download**.

If the transfer times out, choose the FTP server option in the **File is located on** field; the server filename is populated and Prime Infrastructure retries the operation.

Related Topics

View All Controllers in Cisco Prime Infrastructure, on page 3
Apply Controller Changes By Rebooting, on page 7
Download Software to Controllers, on page 8
Replacing Controllers While Retaining the IP Address, on page 19

Download Compressed Web Authorization Login Page Information to Controllers

You can compress the page and image files used for displaying a web authentication login page, known as webauth bundles, and download the file to a controller.

Controllers accept a .tar or .zip file of up to 1 MB in size. The 1 MB limit includes the total size of uncompressed files in the bundle.

To download customized web authentication bundles to a controller, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type > Wireless Controller**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click **Download** > **Download Customized WebAuth**.

Step 4 To download an example login.tar bundle file, click on the preview image displayed, then edit the login.html file and save it as a .tar or .zip file. The file contains the pages and image files required for the web authentication display.

Step 5 Download the .tar or .zip file to the controller.

Step 6 Select where the file is located.

If you select local machine, you can upload either a .zip or .tar file type. Prime Infrastructure converts .zip files to .tar files. If you choose a TFTP server download, you can specify a .tar files only.

Step 7 Complete the required fields, then click **Download**.

If the transfer times out, choose the FTP server option in the **File is located on** field; the server filename is populated and Prime Infrastructure retries the operation.

After Prime Infrastructure completes the download, you are directed to a new page and are able to authenticate.

Related Topics

View All Controllers in Cisco Prime Infrastructure, on page 3
Download Software to Controllers, on page 8
Replacing Controllers While Retaining the IP Address, on page 19

Download Vendor Device Certificates to Controllers

Each wireless device (controller, access point, and client) has its own device certificate. If you want to use your own vendor-specific device certificate, you must download it to the controller.

To download a vendor device certificate to a controller, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	Choose **Inventory** > **Device Management** > **Network Devices**.	
Step 2	Choose **Device Type** > **Wireless Controller** (expand Wireless Controller to select a specific controller series).	
Step 3	Click the **Device Name** of the desired controller.	
Step 4	Click **Configuration** tab.	
Step 5	Choose **System** > **Commands**.	
Step 6	In the**Upload/Download Commands** are, select the transfer protocol.	
Step 7	Select the certificate you want to install and click **Go**.	
Step 8	Fill in the requisite details and click **OK**.	

Related Topics

Download Software to Controllers, on page 8
Replacing Controllers While Retaining the IP Address, on page 19
Download CA Certificates to Controllers, on page 12

Download Vendor Device Certificates to Controllers through TFTP

To download a vendor device certificate via TFTP only, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type > Wireless Controller**.
Step 2 Select the check box(es) of the applicable controller(s).
Step 3 Click **Download > Download Vendor Device Certificate**.
Step 4 Complete the required fields, then click **Download**.

Download CA Certificates to Controllers

Controllers and access points have a certificate authority (CA) certificate that is used to sign and validate device certificates. The controller is shipped with a Cisco-installed CA certificate. This certificate might be used by EAP-TLS and EAP-FAST (when not using PACs) to authenticate wireless clients during local EAP authentication. However, if you want to use your own vendor-specific CA certificate, you must download it to the controller.

To download a vendor CA certificate to the controller, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type > Wireless Controller**.
Step 2 Select the check box(es) of the applicable controller(s).
Step 3 Click **Download** > **Download Vendor Device Certificate**.
Step 4 Complete the required fields, then click **Download**.

Related Topics

Apply Controller Changes By Rebooting, on page 7
Download Software to Controllers, on page 8
Replacing Controllers While Retaining the IP Address, on page 19
View All Controllers in Cisco Prime Infrastructure, on page 3

Configure Network Assurance

Download and Install Device Public Certificates

The Device Public Certificate used for Cisco Wireless Service Assurance is a CA signed certificate signed by Cisco CA server.

Note `cmca2.cer` certificate comes pre-installed in Prime Infrastructure 3.4. You may not need to download and install this certificate.

Step 1 1. Go to https://www.cisco.com/security/pki/ to see the list of Cisco's CAs with their public certificates.

Step 2 Download all the `.cer` files needed for WLCs for which you want to enable Network Assurance on an FTP server.

Example: ftp.abc.com

Step 3 Log in as admin user in the Prime Infrastructure command shell.

Step 4 Copy the certificates from the FTP server to the default repository.

Example: Copying `cmca2` certificate using

```
CLI admin# copy ftp://ftp.abc.com/cmac2.cer disk:/defaultRepo
```

Step 5 Install the CA certificate trust on Prime Infrastructure server for all certificates.

Example: Installing `cmca2.cer` using

```
CLI admin# ncs key importcacert cmca2 cmca2.cer repository defaultRepo
The NCS server is running. Changes will take affect on the next server restart
Importing certificate to trust store
```

Step 6 After installing all the certificates on Prime Infrastructure server, you need to restart it for the certificates to become effective.

Note If the Network Assurance processing reports a device processing error, please look at the ifm_sam.log file to get the Pu sensor device.

Example: Sample `ifm_sam.log` file:

```
2017-10-30 21:34:01,890 [https-jsse-nio-443-exec-1] ERROR logging - IFM-SAM-ERROR: Sensor device X.5
 mentioned below is not properly signed:
**********START*******************************

MIIEdDCCA1ygAwIBAgIKG3upVgAAAA32cTANBgkqhkiG9w0BAQsFADA2MQ4wDAYDVQQKEwVDaXNjbzEkMCIGA1UEAxMbQ2lzY28
Y3R1cmluZyBDQSBTSEEyMB4XDTE1MTAwNzIzMDg1OFoXDTI1MTAwNzIzMTg1OFowgZQxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwp
ybmlhMREwDwYDVQQHEwhTYW4gSm9zZTEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczEjMCEGA1UEAxMaQUlSLUNUODUxMC1LOS1mNG
wYTI3MDAxIDAeBgkqhkiG9w0BCQEWEXN1cHBvcnRAY2lzY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3p
23KzNGSGB1bAV71Y+YmPt+oJR7fVpZI/Vv39ncFcRGCpP0RH6ics9l20j0O/9BLQOwkRJ19d91GoPvCGc9hfU9W9ctRikg3ZPIC
23KzNGSGB1bAV71Y+YmPt+oJR7fVpZI/Vv39ncFcRGCpP0RH6ics9l20j0O/9BLQOwkRJ19d91GoPvCGc9hfU9W9ctRikg3ZPIC
VUjWI/l12zfEAuP9dsXdy29h5I0x19QfTCCjqJUtgTcoDx4QL2WjerZopCmCBlGL5ICFm+SeXADCh9OpZn1lbp4lQIDAQABo4IB
AQDAgWgMB0GA1UdDgQWBBQsA0phzTpk5VNFflYOK2mU8OZnmjAfBgNVHSMEGDAWgBR613mVyrtIK7hVFP2jwA+8pw+WGTBABgNV
3MDWgM6Axhi9odHRwOi8vd3d3LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY3JsL2NtY2EyLmNybDBNBggrBgEFBQcBAQRBMD8wPQ
HMAKGMWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9jZXJ0cy9jbWNhMi5jZXIwPwYJKwYBBAGCNxQCBDIeMABJAE
BuAHQAZQByAG0AZQBkAGkAYQB0AGUATwBmAGYAbABpAG4AZTANBgkqhkiG9w0BAQsFAAOCAQEANOilUIBV7mk3H/rhLGCW7acwi
WOfSZdy0EukZ8gCoKScZyLHp7IEkDGueb4CMJnPi4oJOeDw2xrxS/AkSLWUw5aQ585Qi2J2JXlLAXQ9pgaatyZ0yjm+jkkISwB1
by2ApXdI2HqpNateGZvB0NJ4ww6xnJMIUaSdGl+50CrKWLoCssH2DHp6Qo9a8oTZtM6cG/c5wsjDn0tSfFbt4+3JzUPLnPlAff1
a8pODdVe3BFe44pyMdgGCnVZnqJcevZiWtHMCG5OjaggbBhC0RObGJBxKOAGRgNlUej8hg1hWw==

**********END*******************************

Check the CA Server for device X.509 Certificate is in Prime: 'ncs key listcacerts'.
```

You need to convert the certificate from Base64 to .cer format using tools to see its details and identify the CA server. the CA server used is `Cisco Manufacturing CA (cmca2)`.

Related Topics

Download NA Server CA Certificate to Controllers, on page 16

Generating Self Signed Certificates for Network Assurance , on page 14

Generating Self Signed Certificates for Network Assurance

Cisco Prime Infrastructure supports collection of wireless client information and related events from managed WLCs. This data collection needs an Apache HTTPD running on Prime Infrastructure server that routes the HTTPS requests from a WLC to respective processes. The communication between WLCs and Prime Infrastructure is over HTTPS. This means that PI server's Private Key, Certificate file, and CA-Certificate are needed for communicating with WLCs.

1. When Prime Infrastructure 3.4 is installed, a set of Private Key and X.509 self-signed certificate is automatically generated for WSA Collector and copied to the below locations:
   - **Private Key File location:** `/opt/CSCOlumos/wsa/apache/cert/server.key`
   - **Self Signed Certificate File (X.509 format)location:** `/localdisk/tftp` or `/localdisk/ftp`
   - **CA Certificate file location:** `/opt/CSCOlumos/conf/certs/server_rootcacert.pem`

   You may use your own Private Key, Certificate and CA-Signed certificates by copying the respective files in the locations mentioned above.

   `Example: https://[prime_server_ip]:8080`
2. The Self-Signed certificate uses the IP Address of eth0 interface of Prime Infrastructure server as the Common Name (CN). If you want to continue using the automatically generated certificates, you should configure the WLC's NA Server URL using the eth0 interface's IP Address on Prime Infrastructure server (refer to step 4).`Example: https://[prime_server_ip]:8080`
3. The automatically generated certificates are enough to communicate with WLCs. If you intend to continue using them, then refer below to see how to configure WLCs with these certificates. If you want to generate another set of certificates using Prime Server's host name or another IP Address you can use the following commands:

   Generate Signed Certificate Using IP Address and Host Name

   a. Generate a key file.

   b. Create a Certificate Signing Request(.csr)

   c. Send the CSR to a certificate authority (CA) to obtain an SSL certificate.

   d. Use the key, signed certificate and CA certificate.

   - **Generate a key file using openssl:**

     ```
     openssl genrsa -out apacheserver.key 4096
     ```

   - **Create a Certificate Signing Request(.csr):**

     ```
     openssl req -new -sha256 -key apacheserver.key -config server-csr.conf -out
     apache_signing_request.csr
     ```

     You can give any name for .csr file in the above command. server-csr.conf file may contain following details.

     ```
     [dn]

     C="US"
     ```

```
ST="CA"

L="CA"

O="Cisco Systems"

OU="Prime Infra"

CN="{IP_ADDR}"

[ usr_cert ]

extendedKeyUsage = serverAuth, clientAuth

subjectAltName = @alt_names

[ v3_req ]

extendedKeyUsage = serverAuth, clientAuth

subjectAltName = @alt_names

[ v3_ca ]

extendedKeyUsage = serverAuth, clientAuth

subjectAltName = @alt_names

[alt_names]

DNS = {HOST_NAME}

IP = {IP_ADDR}
```

Note If you want to generate the certificate using Host Name then provide CN="{PI_FQDN}" in server-csr.conf. IP_ADDR is the IP address of Prime Infrastructure server for which you want to generate the keys and certificates and PI_FQDN is the Prime Infrastructure server's fully qualified host name. If the Common Name (CN) provided in the certificate is Prime Infrastructure server's host name, then it has to be DNS resolvable; else you need to provide the IP Address of the Prime Server in the Common Name.

- Send the CSR to a certificate authority (CA) to obtain an SSL certificate.

4. After generating the certificates as mentioned, follow below steps.
   a. Change the format of the Key, Signed Certificate and CA Certificate to .pem and rename as following.
      - Rename Server Certificate as apache_servercert.pem
      - Rename Server Key as apache_serverkey.pem
      - Rename CA Certificate as cacert.pem
   b. Copy the certificates after renaming to `/localdisk/sftp/`
   c. Run following command from admin mode to copy the files to respective locations and to run WSA service with these new certificates.

      ncs run wsa-apache-ca-certs-copy custom

Note If WSA service is not working properly after copying these certificates, then the user can run following command from admin mode to copy the default certificates present on PI.

ncs run wsa-apache-ca-certs-copy default

Related Topics

Download NA Server CA Certificate to Controllers, on page 16

Download NA Server CA Certificate to Controllers

For a WLC to communicate with Prime Infrastructure, the WLC needs to have an NA Server CA Certificate for authentication.

Before you download it, you may have to generate a set of certificates or upload your own to specific locations from where Prime Infrastructure can fetch them; see related links for more information.

Note In an HA setup, when applying a certificate to a WLC, you need to manually add the *ip address* of the secondary server under **Administration** > **Servers** > **TFTP/FTP/SFTP Servers**. You also need to choose the secondary ip from the dropdown list while uploading certificate otherwise the default ip address will be listed as primary after failover in secondary server.

To download the CA certificate to the controller from localdisk under **TFTP location**, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type > Wireless Controller**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click **Download** > **Download NA Server CA Certificate**.

Step 4 Choose the file location, complete the required fields, and then click **Download**.

Download NA Server CA Certificate to Controllers

To download the CA certificate to the controller from **TFTP, FTP, SFTP, or USB location**, follow these steps:

Note In an HA setup, when applying a certificate to a WLC, you need to manually add the *ip address* of the secondary server under **Administration** > **Servers** > **TFTP/FTP/SFTP Servers**. You also need to choose the secondary ip from the dropdown list while uploading certificate otherwise the default ip address will be listed as primary after failover in secondary server.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type > Wireless Controller**.

Step 2 Click the controller on which you want to download the certificate.

Step 3 Click the **Configuration** tab.

Step 4 In the left sidebar manu, click **System** > **Commands**.

Step 5 Choose the file location, and select **Download NA Server CA Certificate** from the drop-down menu.

Note This option is available only for WLCs running AireOS 8.6, 8.7, and 8.8.

Step 6 Click **Go**.

Step 7 Fill the requisite details and click **OK**.

Related Topics

Generating Self Signed Certificates for Network Assurance , on page 14
Configure Network Assurance, on page 128
Apply Controller Changes By Rebooting, on page 7
Download Software to Controllers, on page 8
Replacing Controllers While Retaining the IP Address, on page 19
View All Controllers in Cisco Prime Infrastructure, on page 3

Save Controller Configuration to Device Flash

To save the configuration to flash memory, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click **Configure** > **Save Config to Flash**.

Related Topics

Save Controller Configurations to the Database (Sync), on page 17
Download Software to Controllers, on page 8
Replacing Controllers While Retaining the IP Address, on page 19
Apply Controller Changes By Rebooting, on page 7

Save Controller Configurations to the Database (Sync)

To synchronize the configuration from the controller, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click **Sync**, and **Yes** to proceed.

Related Topics

Save Controller Configuration to Device Flash, on page 17
Download Software to Controllers, on page 8
Replacing Controllers While Retaining the IP Address, on page 19
Apply Controller Changes By Rebooting, on page 7

Discover Existing Templates for Controllers

To discover current templates, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type > Wireless Controller**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click **Configure** > **Discover Templates from Controller**.

The Discover Templates page displays the number of discovered templates, each template type and each template name. The template discovery tool discovers all features that support templates and are discoverable in Cisco WLC.

Step 4 Select the **Enabling this option will create association between discovered templates and the device listed above** check box so that discovered templates are associated to the configuration on the device and are shown as applied on that controller.

The template discovery refreshes the configuration from the controller prior to discovering templates.

Step 5 Click **OK** in the warning dialog box to continue with the discovery.

For the TACACS+ Server templates, the configuration on the controller with same server IP address and port number but different server types are aggregated into one single template with the corresponding Server Types set on the Discovered Template. For the TACACS+ Server templates, the Admin Status on the discovered template reflects the value of Admin Status on the first configuration from the controller with same Server IP address and port number.

View Templates That Have Been Applied to Controllers

You can view all templates currently applied to a specific controller.Prime Infrastructure displays templates applied in the partition only.

To view applied templates, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click **Configure > Templates Applied to a Controller**.

The page displays each applied template name, template type, the date the template was last saved, and the date the template was last applied.

Step 4 Click the template name link to view the template details. See Check Which Configuration Templates Are Used by Controllers and Remove the Associations for more information.

Related Topics

Check Which Configuration Templates Are Used by Controllers and Remove the Associations, on page 5
Replacing Controllers While Retaining the IP Address, on page 19

Replacing Controllers While Retaining the IP Address

When you want to replace an old controller model with a new one without changing the IP address, do the following:

1. Delete the old controller from Cisco Prime Infrastructure and wait for the confirmation that the device was deleted.
2. Replace the controller with the new model in the setup with same IP address.
3. Re-add the IP address to Cisco Prime Infrastructure.

Related Topics

Edit Device Parameters

Modify Controller Properties

To change controller properties such as the device name, location, SNMP parameters, or Telnet/SSH parameters, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices**, then select **Device Type > Wireless Controller**.

Step 2 Select a wireless controller, then click **Edit**.

Step 3 Modify the fields as desired, then click one of the following buttons:

- **Update**
- **Update & Sync**
- **Verify Credentials**
- **Cancel** to return to the previous or default settings.

Change Controller General System Properties from the Network Devices Table

To view the general system parameters for a current controller, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices**, then select **Device Type > Wireless Controller**.

Step 2 Click a Device Name, then click the **Configuration** tab.

Step 3 From the left sidebar menu, choose **System > General - System**. The general system parameters appear. See *Cisco Prime Infrastructure Reference Guide*.

Step 4 Make the required changes, then click **Save**.

Assign Priority to APs When a Controller Fails

When a controller fails, the backup controller configured for the access point suddenly receives a number of Discovery and Join requests. If the controller becomes overloaded, it might reject some of the access points.

By assigning failover priority to an access point, you have some control over which access points are rejected. When the backup controller is overloaded, join requests of access points configured with a higher priority levels take precedence over lower-priority access points.

To configure failover priority settings for access points, you must first enable the AP Failover Priority feature.

To enable the AP Failover Priority feature, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type > Wireless Controller**.

Step 2 Click a Device Name, then click the **Configuration** tab.

Step 3 From the left sidebar menu, choose **General - System**.

Step 4 From the AP Failover Priority drop-down list, choose **Enabled**.

Step 5 To configure an access point failover priority, do the following:

a) Choose **Configuration > Network > Network Devices**, then select an AP Name.

b) From the AP Failover Priority drop-down list, choose the applicable priority (**Low**, **Medium**, **High, Critical**). The default priority is Low.

Configure 802.3 Bridging on a Controller

The controller supports 802.3 frames and applications that use them, such as those typically used for cash registers and cash register servers. However, to make these applications work with the controller, the 802.3 frames must be bridged on the controller.

Support for raw 802.3 frames allows the controller to bridge non-IP frames for applications not running over IP. Only this raw 802.3 frame format is currently supported.

To configure 802.3 bridging using Prime Infrastructure, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type > Wireless Controller**.

Step 2 Click a Device Name, then click the **Configuration** tab.

Step 3 Choose **System > General - System** to access the General page.

Step 4 From the 802.3 Bridging drop-down list, choose **Enable** to enable 802.3 bridging on your controller or **Disable** to disable this feature. The default value is Disable.

Step 5 Click **Save** to confirm your changes.

Configure 802.3 Flow Control on a Controller

Flow control is a technique for ensuring that a transmitting entity, such as a modem, does not overwhelm a receiving entity with data. When the buffers on the receiving device are full, a message is sent to the sending device to suspend the transmission until the data in the buffers has been processed.

By default, flow control is disabled. You can only enable a Cisco switch to receive PAUSE frames but not to send them.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type > Wireless Controller**.

Step 2 Click a Device Name, then click the **Configuration** tab.

Step 3 Choose **System > General - System** to access the General page.

Step 4 Click **Enable** in the 802.3x Flow Control field.

Configure Lightweight AP Protocol Transport Mode from the Network Devices Table

Lightweight Access Point Protocol transport mode indicates the communications layer between controllers and access points. Cisco IOS-based lightweight access points do not support Layer 2 lightweight access point mode. These access points can only be run with Layer 3.

To convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 lightweight access point transport mode using Prime Infrastructure user interface, follow these steps. This procedure causes your access points to go offline until the controller reboots and the associated access points re associate to the controller.

Step 1 Make sure that all controllers and access points are on the same subnet.

You must configure the controllers and associated access points to operate in Layer 2 mode before completing the conversion.

Step 2 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type** > **Wireless Controller**.

Step 3 Click a Device Name, click the **Configuration** tab, then choose **System** > **General - System** to access the General page.

a) Change lightweight access point transport mode to Layer2 and click **Save**.

b) If Prime Infrastructuredisplays the following message, click **OK**:

Example:

```
Please reboot the system for the CAPWAP Mode change to take effect.
```

Step 4 Select the controller, then click **Reboot** > **Reboot Controllers**.

Step 5 Select the **Save Config to Flash** option.

Step 6 After the controller reboots, follow these steps to verify that the CAPWAP transport mode is now Layer 2:

a) Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type** > **Wireless Controller**.
b) Click the device name of the applicable controller.
c) Verify that the current CAPWAP transport mode is Layer2 from the **System** > **General - System** page.

You have completed the CAPWAP transport mode conversion from Layer 3 to Layer 2. The operating system software now controls all communications between controllers and access points on the same subnet.

What is Aggressive Load Balancing?

In routing, load balancing refers to the capability of a router to distribute traffic over all its network ports that are the same distance from the destination address. Good load-balancing algorithms use both line speed and reliability information. Load balancing increases the use of network segments, thus increasing effective network bandwidth.

Aggressive load balancing actively balances the load between the mobile clients and their associated access points.

What is Link Aggregation?

Link aggregation allows you to reduce the number of IP addresses needed to configure the ports on your controller by grouping all the physical ports and creating a link aggregation group (LAG). In a 4402 model, two ports are combined to form a LAG whereas in a 4404 model, all four ports are combined to form a LAG.

You cannot create more than one LAG on a controller.

If LAG is enabled on a controller, the following configuration changes occur:

- Any dynamic interfaces that you have created are deleted in order to prevent configuration inconsistencies in the interface database.
- Interfaces cannot be created with the “Dynamic AP Manager” flag set.

The advantages of creating a LAG include the following:

- Assurance that, if one of the links goes down, the traffic is moved to the other links in the LAG. As long as one of the physical ports is working, the system remains functional.
- You do not need to configure separate backup ports for each interface.
- Multiple AP-manager interfaces are not required because only one logical port is visible to the application.

When you make changes to the LAG configuration, the controller has to be rebooted for the changes to take effect.

Prerequisites for Wireless Management

Because of IPsec operation, management via wireless is only available to operators logging in across WPA, Static WEP, or VPN Pass Through WLANs. Wireless management is not available to clients attempting to log in via an IPsec WLAN.

What is a Mobility Anchor Keep Alive Interval?

You can specify the delay between tries for clients attempting to join another access point. This decreases the time it takes for a client to join another access point following a controller failure because the failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller.

Related Topics

Download Software to Controllers, on page 8
Restore Controller Factory Default Settings, on page 23
Configure the Date and Time on a Controller, on page 23

Restore Controller Factory Default Settings

You can reset the controller configuration to the factory default. This overwrites all applied and saved configuration parameters. You are prompted for confirmation to reinitialize your controller.

All configuration data files are deleted, and upon reboot, the controller is restored to its original non-configured state. This removes all IP configuration, and you need a serial connection to restore its base configuration.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click a Device Name, then click the **Configuration** tab.

Step 3 From the left sidebar menu, choose **System** > **Commands** , and from the Administrative Commands drop-down list, choose **Reset to Factory Default**, and click **Go** to access this page.

Step 4 After confirming configuration removal, you must reboot the controller and select the **Reboot Without Saving** option.

Related Topics

Download Software to Controllers, on page 8
Configure the Date and Time on a Controller, on page 23
Apply Controller Changes By Rebooting, on page 7

Configure the Date and Time on a Controller

You can manually set the current time and date on the controller.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click a Device Name, then click the **Configuration** tab.

Step 3 From the left sidebar menu, choose **System** > **Commands**, and from the Configuration Commands drop-down list choose **Set System Time**, and click **Go**.

Step 4 Modify the required parameters:

- Current Time—Shows the time currently being used by the system.
- Month/Day/Year—Choose the month/day/year from the drop-down list.
- Hour/Minutes/Seconds—Choose the hour/minutes/seconds from the drop-down list.

- Delta (hours)—Enter the positive or negative hour offset from GMT (Greenwich Mean Time).
- Delta (minutes)—Enter the positive or negative minute offset from GMT.
- Daylight Savings—Select to enable Daylight Savings Time.

Upload a Controller's Configuration and Log Files to a TFTP Server

You can upload files from controllers to a local TFTP (Trivial File Transfer Protocol) server. You must enable TFTP to use the Default Server option on the **Administration** > **System Settings** > **Server Settings** page.

Prime Infrastructure uses an integral TFTP server. This means that third-party TFTP servers cannot run on the same workstation as Prime Infrastructure, because the Prime Infrastructure and the third-party TFTP servers use the same communication port.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click a Device Name, then click the **Configuration** tab.

Step 3 From the left sidebar menu, choose **System** > **Commands**.

Step 4 From the **Upload/Download Commands** drop-down list, choose **Upload File from Controller**, then click **Go**.

By default, configuration file encryption is disabled. Uploading configuration file is unsecured without encryption.

Step 5 To enable encryption before uploading files, click the link at the bottom of the Upload File from Controller page.

Step 6 Complete the required fields, then click **OK**. The selected file is uploaded to your TFTP server with the name you specified.

Related Topics

Configure the Date and Time on a Controller, on page 23
Download Software to Controllers, on page 8
Restore Controller Factory Default Settings, on page 23

Download Software To a Controller

You can download configuration files to your controller from a local TFTP (Trivial File Transfer Protocol) server.

Prime Infrastructure uses an integral TFTP server. This means that third-party TFTP servers cannot run on the same workstation as Prime Infrastructure, because the Cisco Prime Infrastructure and the third-party TFTP servers use the same communication port.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type > Wireless Controller**.

Step 2 Click a Device Name, then click the **Configuration** tab.

Step 3 From the left sidebar menu, choose **System > Commands**.

Step 4 From the Upload/Download Commands drop-down list, choose **Download Config**, then click **Go**.

Step 5 Complete the required fields, then click **OK**.

Related Topics

Configure the Date and Time on a Controller, on page 23
Upload a Controller's Configuration and Log Files to a TFTP Server , on page 24
Restore Controller Factory Default Settings, on page 23

Configure Interfaces on a Single Controller

To add an interface:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type > Wireless Controller**.

Step 2 Click a Device Name, then click the **Configuration** tab.

Step 3 From the left sidebar menu, choose **System > Interfaces**.

Step 4 From the Select a command drop-down list, choose **Add Interface** > **Go**.

Step 5 Complete the required fields, then click **Save**.

Related Topics

View the Interfaces on a Controller, on page 25
Delete a Dynamic Interface from a Controller, on page 26
Control User Access to Controllers Using a NAC Appliance, on page 27
Configure Guest Account Access to a Wired Controller, on page 31

View the Interfaces on a Controller

To view the existing interfaces:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click a Device Name, then click the Configuration tab.

Step 3 From the left sidebar menu, choose **System** > **Interfaces**. The following parameters appear:

- Check box—Check box to select the dynamic interface for deletion. Choose **Delete Dynamic Interfaces** from the Select a command drop-down list.
- Interface Name —User-defined name for the interface (for example, Management, Service-Port, Virtual).
- VLAN Id—VLAN identifier between 0 (untagged) and 4096, or N/A.
- Quarantine—Select the check box if the interface has a quarantine VLAN ID configured on it.
- IP Address—IP address of the interface.
- Interface Type—Interface Type: Static (Management, AP-Manager, Service-Port, and Virtual interfaces) or Dynamic (operator-defined interfaces).

- AP Management Status—Status of AP Management interfaces and the parameters include Enabled, Disabled, and N/A. Only the management port can be configured as Redundancy Management Interface port.

Related Topics

View and Manage Controller Interface Groups, on page 27

Delete a Dynamic Interface from a Controller

The dynamic interface cannot be deleted if it has been assigned to any interface group. To delete a dynamic interface:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click a Device Name, then click the **Configuration** tab.

Step 3 From the left sidebar menu, choose **System** > **Interfaces**.

Step 4 Select the check box of the dynamic interface that you want to delete and choose **Delete Dynamic Interfaces** from the **Select a command** drop-down list.

Step 5 Click **OK** to confirm the deletion.

Related Topics

View and Manage Controller Interface Groups, on page 27
View the Interfaces on a Controller, on page 25

Apply Interface Changes to Groups of Controllers Using Controller System Interface Groups

Interface groups are logical groups of interfaces. Interface groups facilitate user configuration where the same interface group can be configured on multiple WLANs or while overriding a WLAN interface per AP group. An interface group can exclusively contain either quarantine or non-quarantine interfaces. An interface can be part of multiple interface groups.

Follow these recommendations while configuring controller system interface groups:

- Ensure that the interface group name is different from the interface name.
- Guest LAN interfaces cannot be part of interface groups

The Interface Groups feature is supported by Cisco Wireless Controller software release 7.0.116.0 and later.

Related Topics

View and Manage Controller Interface Groups, on page 27
Control User Access to Controllers Using a NAC Appliance, on page 27

View and Manage Controller Interface Groups

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click on a Device Name, then click the **Controller** tab.

Step 3 From the left sidebar menu, choose **System** > **Interface Groups>**.

The following parameters appear:

- Name—User-defined name for the interface group (For example, group1, group2).
- Description—(Optional) Description for the Interface Group.
- Interfaces—Count of the number of interfaces belonging to the group.

Step 4 To view the existing Interface groups, Click the Interface Group Name link.

The Interface Groups Details page appears with the Interface group details as well as the details of the Interfaces that form part of that particular Interface group.

Step 5 To add an interface group, do the following:

a) From the Select a command drop-down list, choose **Add Interface Group** and click **Go**.
b) Complete the required fields, then click **Add**.
c) The Interface dialog box appears.
d) Select the interfaces that you want to add to the group, and click **Select**.

Step 6 To delete an interface group, do the following:

a) From the Select a command drop-down list, choose **Delete Interface Group**, and click **Go.**

Note You cannot delete interface groups that are assigned to WLANs, AP groups, Foreign Controller Mapping for WLANs, WLAN templates and AP group templates.

b) Click **OK** to confirm the deletion.

Step 7 To remove an Interface from the Interface group, from the Interface Group page, select the Interface and click **Remove**.

Step 8 Click **Save** to confirm the changes made.

Related Topics

Apply Interface Changes to Groups of Controllers Using Controller System Interface Groups, on page 26
Control User Access to Controllers Using a NAC Appliance, on page 27

Control User Access to Controllers Using a NAC Appliance

The Cisco Network Admission Control (NAC) appliance, also known as Cisco Clean Access (CCA), is a Network Admission Control (NAC) product that allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network. It identifies whether machines are compliant with security policies and repairs vulnerabilities before permitting access to the network. The NAC appliance is available in two modes: in-band and out-of-band. Customers can deploy both modes if desired, each geared toward certain types of access (in-band for supporting wireless users and out-of-band for supporting wired users, for example).

Related Topics

Prerequisites for Using SNMP NAC, on page 28
Configure SNMP NAC on a Controller, on page 29

Prerequisites for Using SNMP NAC

Follow these guidelines when using SNMP NAC out-of-band integration:

- The NAC appliance supports up to 3500 users, and the controller supports up to 5000 users. Therefore, multiple NAC appliances might need to be deployed.
- Because the NAC appliance supports static VLAN mapping, you must configure a unique quarantine VLAN for each interface configured on the controller. For example, you might configure a quarantine VLAN of 110 on controller 1 and a quarantine VLAN of 120 on controller 2. However, if two WLANs or guest LANs use the same distribution system interface, they must use the same quarantine VLAN, provided they have one NAC appliance deployed in the network. The NAC appliance supports unique quarantine-to-access VLAN mapping.
- For posture reassessment based on session expiry, you must configure the session timeout on both the NAC appliance and the WLAN, making sure that the session expiry on the WLAN is greater than that on the NAC appliance.
- When a session timeout is configured on an open WLAN, the timing out of clients in the Quarantine state is determined by the timer on the NAC appliance. Once the session timeout expires for WLANs using web authentication, clients deauthenticate from the controller and must perform posture validation again.
- NAC out-of-band integration is supported only on WLANs configured for FlexConnect central switching. It is not supported for use on WLANs configured for FlexConnect local switching.
- If you want to enable NAC on an access point group VLAN, you must first enable NAC on the WLAN. Then you can enable or disable NAC on the access point group VLAN. If you ever decide to disable NAC on the WLAN, be sure to disable it on the access point group VLAN as well.
- NAC out-of-band integration is not supported for use with the WLAN AAA override feature.
- All Layer 2 and Layer 3 authentication occurs in the quarantine VLAN. To use external web authentication, you must configure the NAC appliance to allow HTTP traffic to and from external web servers and to allow the redirect URL in the quarantine VLAN.

For more details, please refer to Cisco NAC Appliance Configuration.

Prerequisites for Using RADIUS NAC

Follow these guidelines when using RADIUS NAC:

- RADIUS NAC is available only for WLAN with 802.1x/WPA/WPA2 Layer 2 security.
- RADIUS NAC cannot be enabled when FlexConnect local switching is enabled.
- AAA override should be enabled to configure RADIUS NAC.

Related Topics

Control User Access to Controllers Using a NAC Appliance, on page 27

Configure SNMP NAC on a Controller

To configure SNMP NAC out-of-band integration, follow this workflow:

1. Configure the quarantine VLAN for a dynamic interface—The NAC appliance supports static VLAN mapping, and you must configure a unique quarantine VLAN for each interface that is configured on the controller.
2. Configure NAC out-of-band support on a WLAN or guest LAN—To enable NAC support on an access point group VLAN, you must first enable NAC on the WLAN or guest LAN.
3. Configure NAC Out-of-band support for a specific AP group—To configure NAC out-of-band support for specific access point groups.

Related Topics

Configure the Quarantine VLANs (SNMP NAC), on page 29
Enable NAC on the WLAN or Guest LAN (SNMP NAC), on page 29
Configure NAC Out-of-Band Support for an AP Group (SNMP NAC), on page 30

Configure the Quarantine VLANs (SNMP NAC)

To configure the quarantine VLAN for a dynamic interface:

Step 1 Choose **Configuration** > **Network** > **Network Devices**Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Choose which controller you are configuring for out-of-band integration by clicking it in the IP Address column.

Step 3 Choose **System** > **Interfaces** from the left sidebar menu.

Step 4 Click the Interface Name.

Step 5 Choose **Add Interface** from the **Select a command** drop-down list and click **Go**.

Step 6 In the **Interface Name** text box, enter a name for this interface, such as “quarantine.”

Step 7 In the **VLAN ID** text box, enter a non-zero value for the access VLAN ID, such as “10.”

Step 8 Select the **Quarantine** check box if the interface has a quarantine VLAN ID configured on it.

Step 9 Configure any remaining fields for this interface, such as the IP address, netmask, and default gateway.

Note To avoid issues when adding the wireless controller to Prime Infrastructure, the Dynamic Interface should not be in the same subnet as Prime Infrastructure.

Step 10 Enter an IP address for the primary and secondary DHCP server.

Step 11 Click **Save**.

Related Topics

Enable NAC on the WLAN or Guest LAN (SNMP NAC), on page 29
Configure NAC Out-of-Band Support for an AP Group (SNMP NAC), on page 30

Enable NAC on the WLAN or Guest LAN (SNMP NAC)

To configure NAC out-of-band support on a WLAN or guest LAN, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click on a Device Name.

Step 3 Choose **WLANs > WLAN** from the left sidebar menu.

Step 4 Choose **Add a WLAN** from the **Select a command** drop-down list, and click **Go**.

Step 5 If you have a template established that you want to apply to this controller, choose the guest LAN template name from the drop-down list. Otherwise, click the **click here** link to create a new template.

Step 6 Click the **Advanced** tab.

Step 7 To configure SNMP NAC support for this WLAN or guest LAN, choose **SNMP NAC** from the drop-down list. To disable SNMP NAC support, choose **None** from the **NAC Stage** drop-down list, which is the default value.

Step 8 Click **Apply** to commit your changes.

Related Topics

Configure NAC Out-of-Band Support for an AP Group (SNMP NAC), on page 30
Configure Guest Account Access to a Wired Controller, on page 31

Configure NAC Out-of-Band Support for an AP Group (SNMP NAC)

To configure NAC out-of-band support for a specific AP group, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 Choose **WLANs** > **AP Groups VLAN** from the left sidebar menu to open the AP Groups page.

Step 4 Click the name of the desired AP group.

Step 5 From the Interface Name drop-down list, choose the quarantine enabled interface.

Step 6 To configure SNMP NAC support for this AP group, choose **SNMP NAC** from the Nac State drop-down list. To disable NAC out-of-band support, choose **None** from the Nac State drop-down list, which is the default value.

Step 7 Click **Apply** to commit your changes.

Related Topics

Enable NAC on the WLAN or Guest LAN (SNMP NAC), on page 29
Configure Guest Account Access to a Wired Controller, on page 31
Configure the Quarantine VLANs (SNMP NAC), on page 29

View NAC State for a Network Client or User

To see the current state of the client (either Quarantine or Access), follow these steps:

Step 1 Choose **Monitor** > **Monitoring Tools** > **Clients and Users** to open the Clients. Perform a search for clients.

Step 2 Click the MAC address of the desired client to open the Clients > Detail page. The NAC state appears as access, invalid, or quarantine in the Security Information section.

Related Topics

Configure SNMP NAC on a Controller, on page 29

Configure Guest Account Access to a Wired Controller

Wired Guest Access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or specific ports in a conference room.

Like wireless guest user accounts, wired guest access ports are added to the network using the Lobby Ambassador feature. Wired Guest Access can be configured in a standalone configuration or in a dual controller configuration employing an anchor and foreign controller. This latter configuration is used to further isolate wired guest access traffic but is not required for deployment of wired guest access.

Wired Guest Access ports initially terminate on a Layer 2 access switch or switch port which is configured with VLAN interfaces for wired guest access traffic. The wired guest traffic is then trunked from the access switch to a wireless LAN controller. This controller is configured with an interface that is mapped to a wired guest access VLAN on the access switch.

If two controllers are being used, the controller (foreign) that receives the wired guest traffic from the switch then forwards the wired guest traffic to an anchor controller that is also configured for wired guest access. After successful hand off of the wired guest traffic to the anchor controller, a bidirectional Ethernet over IP (EoIP) tunnel is established between the foreign and anchor controllers to handle this traffic.

Although wired guest access is managed by anchor and foreign anchors when two controllers are deployed, mobility is not supported for wired guest access clients. In this case, DHCP and web authentication for the client are handled by the anchor controller.

You can specify how much bandwidth a wired guest user is allocated in the network by configuring and assigning a role and bandwidth contract.

Related Topics

- Configure and Enable Wired Guest User Access: Workflow

Configure and Enable Wired Guest User Access: Workflow

To configure and enable the wired guest user access, follow this workflow:

1. Configure a dynamic interface (VLAN) for wired guest access—Create a dynamic interface to enable the wired guest user access.
2. Configure a wired LAN for guest user access—Configure a new LAN, which is a guest LAN.

Related Topics

Configure a Dynamic Interface for Wired Guest User Access, on page 32
Configure a Wired LAN for Guest User Access, on page 32

Configure a Dynamic Interface for Wired Guest User Access

To configure and enable a dynamic interface (VLAN) for wired guest user access on the network:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 Choose **System > Interfaces** from the left sidebar menu.

Step 4 Choose **Add Interface** from the Select a command drop-down list, and click **Go**.

Step 5 Complete the required fields.

Step 6 Click **Save**.

Related Topics

Configure and Enable Wired Guest User Access: Workflow, on page 31

Configure a Wired LAN for Guest User Access

To configure a wired LAN for guest user access:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type> Wireless Controller**.

Step 2 Click on a Device Name.

Step 3 To configure a wired LAN for guest user access, choose **WLANs > WLAN configuration** from the left sidebar menu.

Step 4 Choose **Add a WLAN** from the Select a command drop-down list, and click **Go**.

Step 5 If you have a template established that you want to apply to this controller, choose the guest LAN template name from the drop-down list. Otherwise, click the **click here** link to create a new template.

Step 6 In the WLAN > New Template general page, enter a name in the **Profile Name** text box that identifies the guest LAN. Do not use any spaces in the name entered.

Step 7 Select the **Enabled** check box for the WLAN Status field.

Step 8 From the **Ingress Interface** drop-down list, choose the VLAN that you created in Step 3. This VLAN provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 9 From the **Egress Interface** drop-down list, choose the name of the interface. This WLAN provides a path out of the controller for wired guest client traffic.If you have only one controller in the configuration, choose **management** from the Egress Interface drop-down list.

Step 10 Click the **Security > Layer 3** tab to modify the default security policy (web authentication) or to assign WLAN specific web authentication (login, logout, login failure) pages and the server source.

a) To change the security policy to passthrough, select the **Web Policy** check box and select the **Passthrough** radio button. This option allows users to access the network without entering a username or password.

An Email Input check box appears. Select this check box if you want users to be prompted for their e-mail address when attempting to connect to the network.

b) To specify custom web authentication pages, unselect the Global WebAuth Configuration **Enabled** check box.

When the Web Auth Type drop-down list appears, choose one of the following options to define the web login page for the wireless guest users:

Default Internal—Displays the default web login page for the controller. This is the default value.

Customized Web Auth—Displays custom web login, login failure, and logout pages. When the customized option is selected, three separate drop-down lists for login, login failure, and logout page selection appear. You do not need to define a customized page for all three of the options. Choose **None** from the appropriate drop-down list if you do not want to display a customized page for that option.

External—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

You can select specific RADIUS or LDAP servers to provide external authentication in the Security > AAA pane. The RADIUS and LDAP external servers must be already configured to have selectable options in the Security > AAA pane. You can configure these servers on the RADIUS Authentication Servers, TACACS+ Authentication Servers page, and LDAP Servers page.

Step 11 If you selected External as the Web Authentication Type, choose **Security > AAA** and choose up to three RADIUS and LDAP servers using the drop-down lists.

Step 12 Click **Save**.

Step 13 Repeat this process if a second (anchor) controller is being used in the network.

Related Topics

Configure and Enable Wired Guest User Access: Workflow, on page 31

Configure a Guest LAN Ingress Interface on a Controller

To create an Ingress interface:

Step 1 Choose **Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller**.

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 Choose **System > Interfaces** from the left sidebar menu.

Step 4 Choose **Add Interface** from the Select a command drop-down list, and click **Go**.

Step 5 In the Interface Name text box, enter a name for this interface, such as guestinterface.

Step 6 Enter a VLAN identifier for the new interface.

Step 7 Select the **Guest LAN** check box.

Step 8 Enter the primary and secondary port numbers.

Step 9 Click **Save**.

Related Topics

Configure a Guest LAN Egress Interface on a Controller, on page 34

Configure a Guest LAN Egress Interface on a Controller

To create an Egress interface:

Step 1 Choose **Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller**.

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 Choose **System > Interfaces** from the left sidebar menu.

Step 4 Choose **Add Interface** from the Select a command drop-down list, and click **Go**.

Step 5 In the Interface Name text box, enter a name for this interface, such as quarantine.

Step 6 In the vlan Id text box, enter a non-zero value for the access VLAN ID, such as 10.

Step 7 Select the **Quarantine** check box and enter a non-zero value for the Quarantine VLAN identifier, such as 110.

You can have NAC-support enabled on the WLAN or guest WLAN template Advanced tab for interfaces with Quarantine enabled.

Step 8 Enter the IP address, Netmask, and Gateway information.

Step 9 Enter the primary and secondary port numbers.

Step 10 Provide an IP address for the primary and secondary DHCP server.

Step 11 Configure any remaining fields for this interface, and click **Save**.

You are now ready to create a wired LAN for guest access.

Related Topics

Configure a Guest LAN Ingress Interface on a Controller, on page 33

Configure a Network Route on a Controller Service Port

The Network Route page enables you to add a route to the controller service port. This route allows you to direct all Service Port traffic to the designated management IP address.

Related Topics

View Existing Controller Network Routes, on page 34
Add Network Routes to a Controller, on page 35

View Existing Controller Network Routes

To view existing network routes:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**. .

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 Choose **System** > **Network Route** > from the left sidebar menu. The following parameters appear:

- IP Address—The IP address of the network route.
- IP Netmask—Network mask of the route.
- Gateway IP Address—Gateway IP address of the network route.

Related Topics

Configure a Network Route on a Controller Service Port, on page 34

Add Network Routes to a Controller

To add a network route, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 Choose **System > Network Route** from the left sidebar menu.

Step 4 From the Select a command drop-down list, choose **Add Network Route**.

Step 5 Click **Go**.

Step 6 Complete the required fields, then click **Save**.

Related Topics

Configure a Network Route on a Controller Service Port, on page 34
Configure the Date and Time on a Controller, on page 23

View a Controller's STP Parameters

Spanning Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

To view or manage current STP parameters:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the **Device Groups** menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click on a Device Name, then click the **Controller** tab.

Step 3 Choose **System** > **Spanning Tree Protocol** from the left sidebar menu. The Spanning Tree Protocol page displays the following parameters:

- Protocol Spec—The current protocol specification.
- Admin Status—Select this check box to enable.
- Priority—The numerical priority number of the ideal switch.
- Maximum Age (seconds)—The amount of time (in seconds) before the received protocol information recorded for a port is discarded.

- Hello Time (seconds)—Determines how often (in seconds) the switch broadcasts its hello message to other switches.
- Forward Delay (seconds)—The time spent (in seconds) by a port in the learning/listening states of the switches.

Related Topics

Configure a Network Route on a Controller Service Port, on page 34
Change Controller General System Properties from the Network Devices Table, on page 19

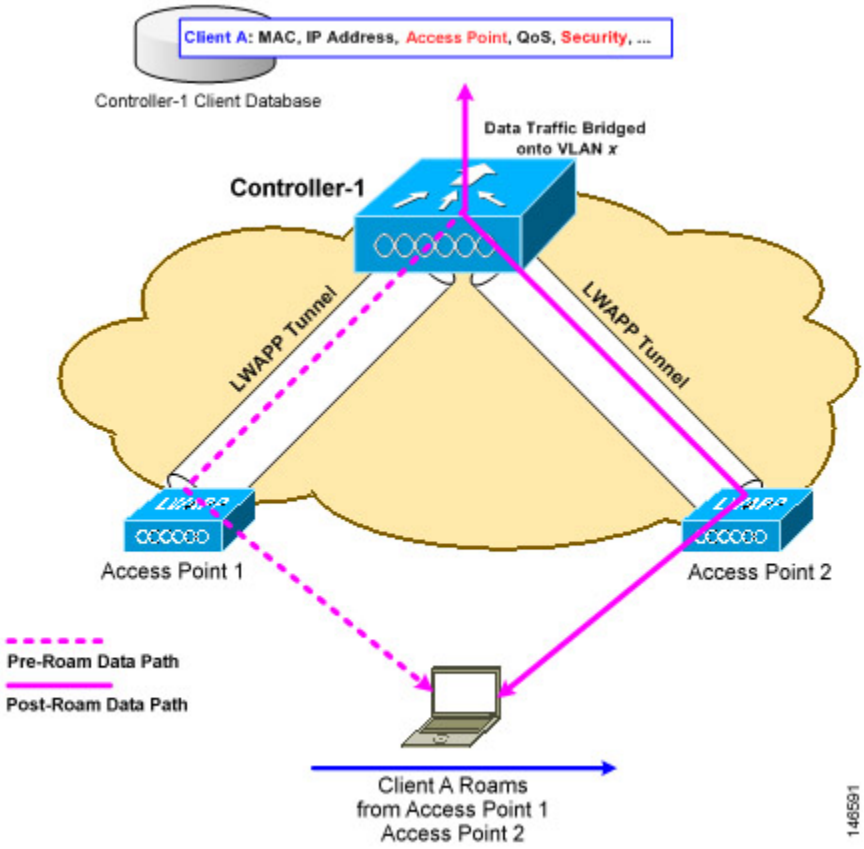
What is Mobility?

Mobility, or roaming, is an ability of a wireless client to maintain its association seamlessly from one access point to another, securely and with as little latency as possible, in a wireless network. When a wireless client is associated to and authenticated by an access point, a controller places an entry for that client in its client database. This entry includes the MAC and IP addresses of the client, security context and associations, quality of service (QoS) contexts, the WLANs, and the associated access point. The controller uses this information to forward frames and manage traffic to and from the wireless client.

What is Intra-Controller Roaming?

When the wireless client moves its association from one access point to another, the controller simply updates the client database with the newly associated access point. If necessary, new security context and associations are established as well. The folowing figure illustrates a wireless client roaming from one access point to another when both access points are connected to the same controller. Figure 146591

Figure 1: Intra-Controller Roaming



Related Topics

What is Mobility?, on page 36
What are Mobility Groups?, on page 40
What is Inter-Controller Roaming?, on page 37

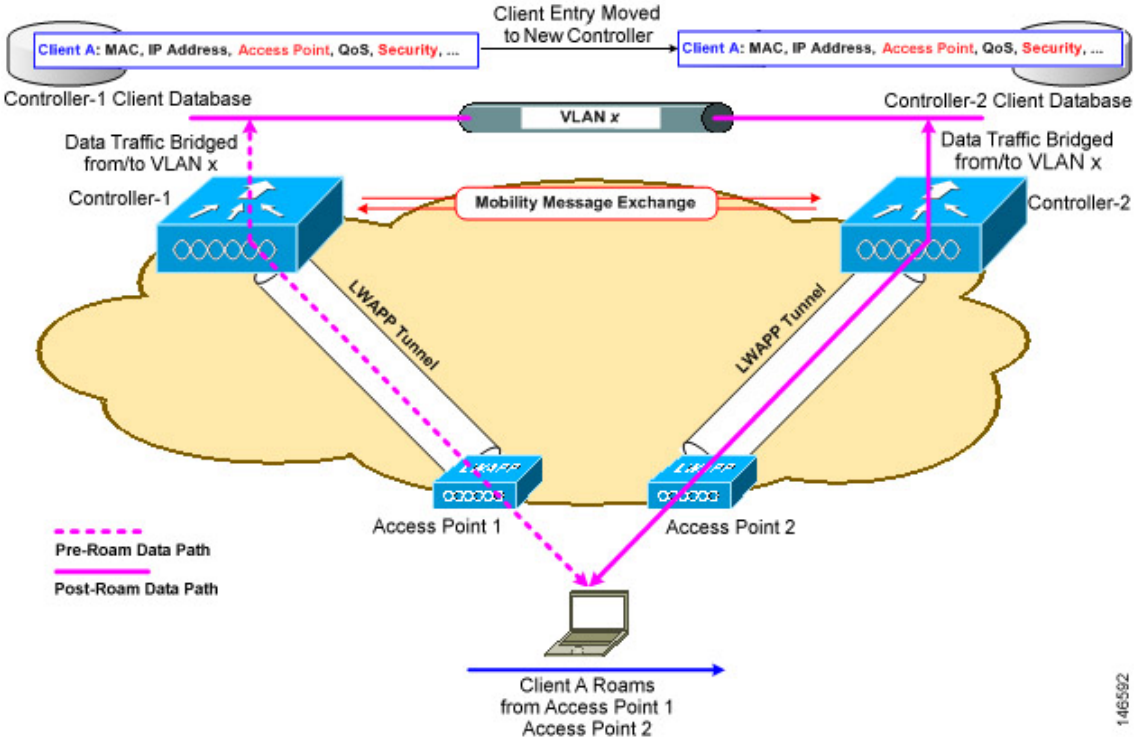
What is Inter-Controller Roaming?

When a client roams from an access point connected to one controller to an access point connected to a different controller, the process also varies based on whether the controllers are operating on the same subnet. The following figure illustrates *inter-controller roaming* , which occurs when the wireless LAN interfaces of a controller are on the same IP subnet.

When the client is associated to an access point connected to a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database entry is updated for the new access point. This process remains invisible to the user.

All clients configured with 802.1X/Wi-Fi Protected Access (WPA) security complete a full authentication to comply with the IEEE standard.

Figure 2: Inter-Controller Roaming



Related Topics

What is Mobility?, on page 36
What are Mobility Groups?, on page 40
What is Intra-Controller Roaming?, on page 36
Prerequisites for Adding Controllers to Mobility Groups, on page 41

What is Inter-Subnet Roaming?

Inter-subnet roaming is similar to inter-controller roaming in that the controllers exchange mobility messages on how the client roams. However, instead of moving the client database entry to the new controller, the original controller marks the client with an “Anchor” entry in its own client database. The database entry is copied to the new controller client database and marked with a “Foreign” entry in the new controller. The roam remains invisible to the wireless client, and the client maintains its original IP address.

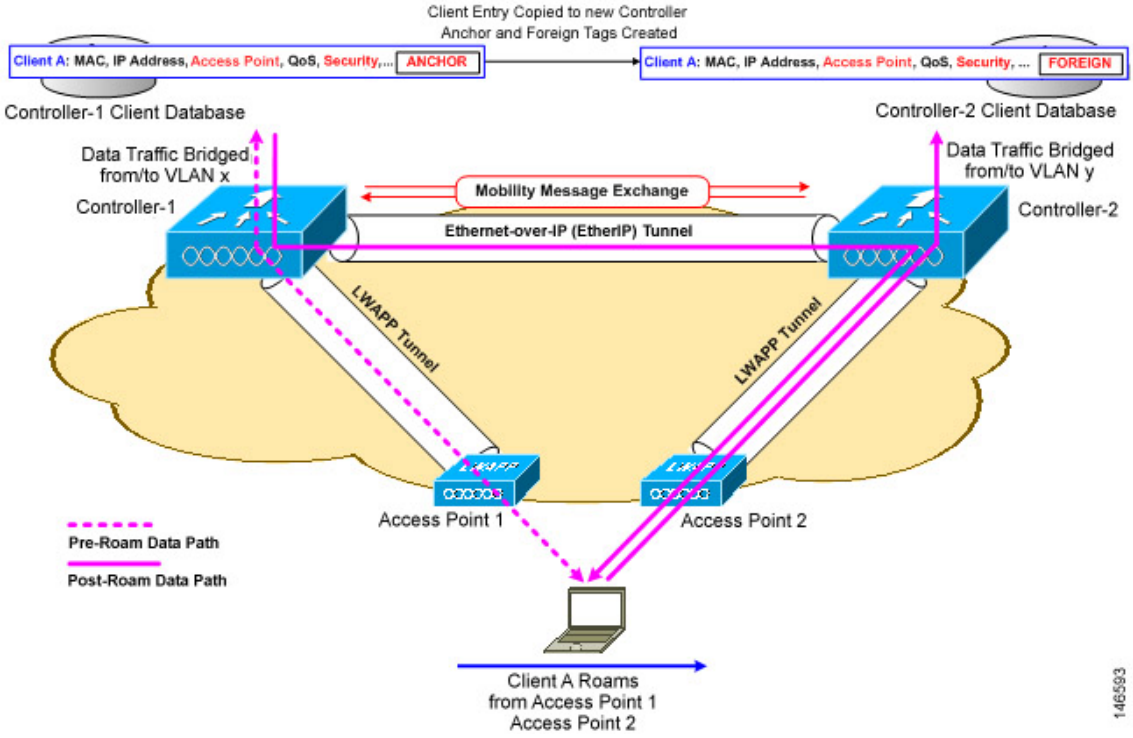
After an inter-subnet roam, data flows in an asymmetric traffic path to and from the wireless client. Traffic from the client to the network is forwarded directly into the network by the foreign controller. Traffic to the client arrives at the anchor controller, which forwards the traffic to the foreign controller in an EtherIP tunnel. The foreign controller then forwards the data to the client. If a wireless client roams to a new foreign controller, the client database entry is moved from the original foreign controller to the new foreign controller, but the original anchor controller is always maintained. If the client moves back to the original controller, it becomes local again.

In inter-subnet roaming, WLANs on both anchor and foreign controllers need to have the same network access privileges and no source-based routing or source-based firewalls in place. Otherwise, the clients might have network connectivity problems after the handoff.

Inter-subnet roaming does not support multicast traffic such as one used by Spectralink phones while using push-to-talk.

The following figure 146593 illustrates *inter-subnet roaming* , which occurs when the wireless LAN interfaces of a controller are on different IP subnets.

Figure 3:



Related Topics

What is Mobility?, on page 36
What are Mobility Groups?, on page 40
What is Intra-Controller Roaming?, on page 36
What is Inter-Controller Roaming?, on page 37
Prerequisites for Adding Controllers to Mobility Groups, on page 41

What is Symmetric Tunneling?

With symmetric mobility tunneling, the controller provides inter-subnet mobility for clients roaming from one access point to another within a wireless LAN. The client traffic on the wired network is directly routed by the foreign controller. If a router has Reverse Path Filtering (RPF) enabled (which provides additional checks on incoming packets), the communication is blocked. Symmetric mobility tunneling allows the client traffic to reach the controller designated as the anchor, even with RPF enabled. All controllers in a mobility group should have the same symmetric tunneling mode.

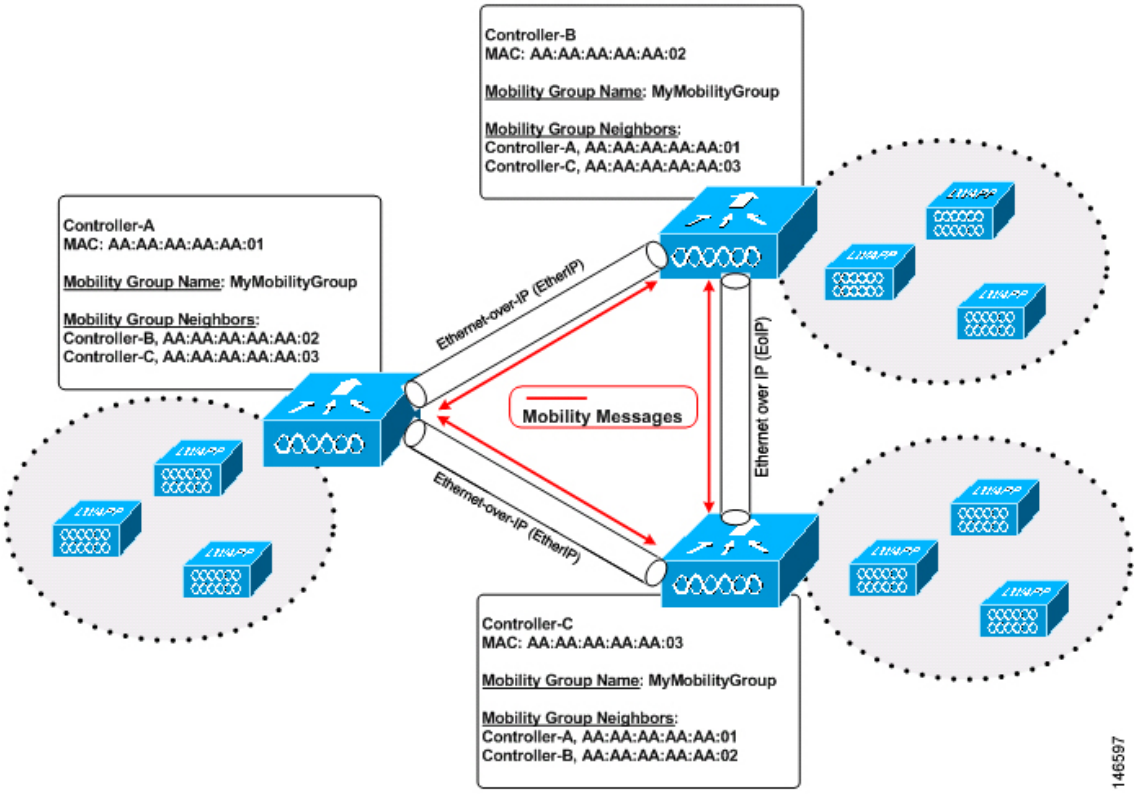
With this feature, the time it takes for a client to join another access point following a controller failure is decreased because a failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller.

What are Mobility Groups?

A set of controllers can be configured as a *mobility group* to allow seamless client roaming within a group of controllers. This enables multiple controllers to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers can share the context and state of clients and controller loading information With this information, the network can support inter-controller wireless LAN roaming and controller redundancy. Clients do not roam across mobility groups

The following figure shows an example of a mobility group.

Figure 4: Single Mobility Group



As shown in the above figure, each controller is configured with a list of the other members of the mobility group. Whenever a new client joins a controller, the controller sends out a unicast message to all of the controllers in the mobility group. The controller to which the client was previously connected passes on the status of the client. All mobility exchange traffic between controllers is carried over a CAPWAP tunnel.

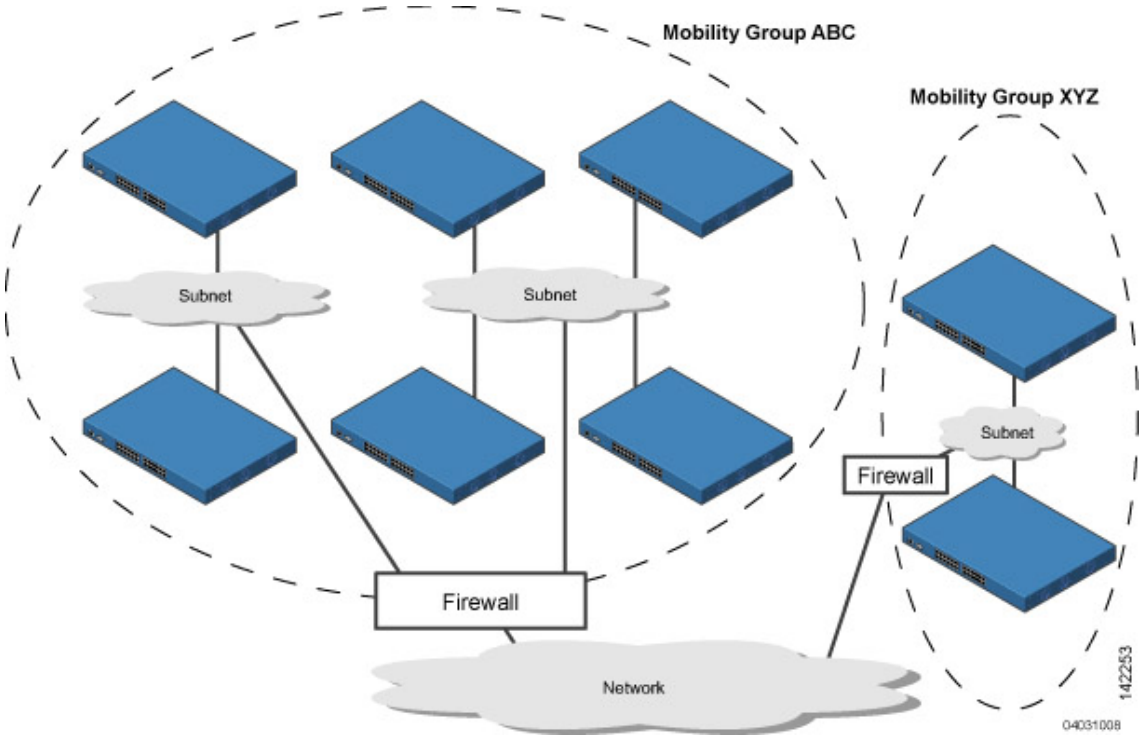
Examples:

1. A 4404-100 controller supports up to 100 access points. Therefore, a mobility group consisting of 24 4404-100 controllers supports up to 2400 access points (24 * 100 = 2400 access points).
2. A 4402-25 controller supports up to 25 access points, and a 4402-50 controller supports up to 50 access points. Therefore, a mobility group consisting of 12 4402-25 controllers and 12 4402-50 controllers supports up to 900 access points (12 * 25 + 12 * 50 = 300 + 600 = 900 access points).

Mobility groups enable you to limit roaming between different floors, buildings, or campuses in the same enterprise by assigning different mobility group names to different controllers within the same wireless

network. The following figure shows the results of creating distinct mobility group names for two groups of controllers.

Figure 5: Two Mobility Groups



The controllers in the ABC mobility group recognize and communicate with each other through their access points and through their shared subnets. The controllers in the ABC mobility group do not recognize or communicate with the XYZ controllers, which are in a different mobility group. Likewise, the controllers in the XYZ mobility group do not recognize or communicate with the controllers in the ABC mobility group. This feature ensures mobility group isolation across the network. Clients might roam between access points in different mobility groups, provided they can detect them. However, their session information is not carried between controllers in different mobility groups.

Related Topics

Prerequisites for Adding Controllers to Mobility Groups, on page 41
How Controller Mobility Group Messaging Works, on page 42

Prerequisites for Adding Controllers to Mobility Groups

Before you add controllers to a mobility group, you must verify that the following prerequisites are met for all controllers that are to be included in the group:

- All controllers must be configured for the same CAPWAP transport mode (Layer 2 or Layer 3).
- IP connectivity must exist between the management interfaces of all controllers.
- All controllers must be configured with the same mobility group name.
- All controllers must be configured with the same virtual interface IP address.

- You must have gathered the MAC address and IP address of every controller that is to be included in the mobility group. This information is necessary because you will be configuring all controllers with the MAC address and IP address of all the other mobility group members.
- If it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, both controllers should be in the same mobility group.

Related Topics

What are Mobility Groups?, on page 40
How Controller Mobility Group Messaging Works, on page 42

How Controller Mobility Group Messaging Works

The controller provides inter-subnet mobility for clients by sending mobility messages to other member controllers. There can be up to 72 members in the list with up to 24 in the same mobility group. In Cisco Prime Infrastructure Prime Infrastructure and controller software releases 5.0, two improvements have been made to mobility messaging, each of which is especially useful when sending messages to the full list of mobility members:

- Sending Mobile Announce messages within the same group first and then to other groups in the list

The controller sends a Mobile Announce message to members in the mobility list each time a new client associates to it. In the software releases prior to 5.0, the controller sends this message to all members in the list irrespective of the group to which they belong. However, in the software release 5.0, the controller sends the message only to those members that are in the same group as the controller and then includes all of the other members while sending retries.

- Sending Mobile Announce messages using multicast instead of unicast

In Cisco Prime Infrastructure and controller software releases prior to 5.0, the controller might be configured to use multicast to send the mobile announce messages, which requires sending a copy of the messages to every mobility member. This behavior is not efficient because many messages (such as Mobile Announce, Pairwise Primary Key (PPK) Update, AP List Update, and Intrusion Detection System (IDS) Shun) are meant for all members in the group. In Cisco Prime Infrastructure and controller software releases 5.0, the controller uses multicast mode to send the Mobile Announce messages. This behavior allows the controller to send only one copy of the message to the network, which destines it to the multicast group containing all the mobility members. To derive the maximum benefit from multicast messaging, We recommend that it be enabled or disabled on all group members.

Related Topics

What are Mobility Groups?, on page 40
Prerequisites for Adding Controllers to Mobility Groups, on page 41
Configuring Mobility Groups: Workflow, on page 42

Configuring Mobility Groups: Workflow

Whenever you configure a Mobility Group, follow this workflow:

1. Make sure you have gathered the information you need and that the participating controller are properly configured, as explained in Prerequisites for Adding Controllers to Mobility Groups, on page 41.
2. Add individual controllers to the Mobility Group. You may need to add them manually if no Mobility Groups exist or no controllers are listed when you try to add them from the **Configuration** > **Network** > **Network Devices** page.

3. Set the scale and messaging parameters for the Mobility Group.

Prerequisites for Adding Controllers to Mobility Groups

Before you add controllers to a mobility group, you must verify that the following prerequisites are met for all controllers that are to be included in the group:

- All controllers must be configured for the same CAPWAP transport mode (Layer 2 or Layer 3).
- IP connectivity must exist between the management interfaces of all controllers.
- All controllers must be configured with the same mobility group name.
- All controllers must be configured with the same virtual interface IP address.
- You must have gathered the MAC address and IP address of every controller that is to be included in the mobility group. This information is necessary because you will be configuring all controllers with the MAC address and IP address of all the other mobility group members.
- If it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, both controllers should be in the same mobility group.

Related Topics

What are Mobility Groups?, on page 40
How Controller Mobility Group Messaging Works, on page 42

View the Controllers That Belong to a Mobility Group

To view current mobility group members:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 Choose **System** > **Mobility Groups** from the left sidebar menu.

Related Topics

Add Controllers to a Mobility Group from the Network Devices Table, on page 43

Add Controllers to a Mobility Group from the Network Devices Table

To add a mobility group member from a list of existing controllers:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 Choose **System** > **Mobility Groups** from the left sidebar menu.

Step 4 From the Select a command drop-down list, choose **Add Group Members**.

Step 5 Click **Go**.

Step 6 Select the check box(es) for the controller to be added to the mobility group.

Step 7 Click **Save**.

Step 8 If no controllers are listed in Step 6, then you can manually add one by doing the following:

a) Click the **click here** link from the Mobility Group Member details page.
b) In the **Member MAC Address** text box, enter the MAC address of the controller to be added.
c) In the **Member IP Address** text box, enter the management interface IP address of the controller to be added.

If you are configuring the mobility group in a network where Network Address Translation (NAT) is enabled, enter the IP address sent to the controller from the NAT device rather than the controller management interface IP address. Otherwise, mobility fails among controllers in the mobility group.

d) Enter the multicast group IP address to be used for multicast mobility messages in the Multicast Address text box. The local mobility member group address must be the same as the local controller group address.
e) In the **Group Name** text box, enter the name of the mobility group.
f) Click **Save**.

Repeat the above steps for the remaining Cisco Wireless Controller devices.

Related Topics

View the Controllers That Belong to a Mobility Group, on page 43

Configure Multicast Mode for Messages to Mobility Members

Before You Begin

You must configure Mobility Groups prior setting up the mobility scalability parameters.

To set the mobility message parameters:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the Device Name of a controller whose software version is 5.0 or later.

Step 3 From the left sidebar menu, choose **System** > **General**.

Step 4 From the Multicast Mobility Mode drop-down list, specify if you want to enable or disable the ability for the controller to use multicast mode to send Mobile Announce messages to mobility members.

Step 5 If you enabled multicast messaging by setting multicast mobility mode to enabled, you must enter the group IP address at the Mobility Group Multicast-address field to begin multicast mobility messaging. You must configure this IP address for the local mobility group but it is optional for other groups within the mobility list. If you do not configure the IP address for other (non-local) groups, the controllers use unicast mode to send mobility messages to those members.

Step 6 Click **Save**.

Related Topics

Configure Multicast Mode and IGMP Snooping on a Controller, on page 54
Change Controller General System Properties from the Network Devices Table, on page 19

Add an NTP Server to a Controller

To add a new NTP Server:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the Device Name of the applicable controller.

Step 3 From the left sidebar menu, choose **System > Network Time Protocol**.

Step 4 From the Select a command drop-down list, choose **Add NTP Server**.

Step 5 Click **Go**.

Step 6 From the **Select a template to apply to this controller** drop-down list, choose the applicable template to apply to this controller.

Related Topics

Change Controller General System Properties from the Network Devices Table, on page 19

Configure Controllers for Mesh Network Background Scanning

Background scanning allows Cisco Aironet 1510 Access Points to actively and continuously monitor neighboring channels for more optimal paths and parents. Because the access points are searching on neighboring channels as well as the current channel, the list of optimal alternate paths and parents is greater.

Identifying this information prior to the loss of a parent results in a faster transfer and the best link possible for the access points. Additionally, access points might switch to a new channel if a link on that channel is found to be better than the current channel in terms of fewer hops, stronger signal-to-noise ratio (SNR), and so on.

Background scanning on other channels and data collection from neighbors on those channels are performed on the primary backhaul between two access points:

The primary backhaul for 1510s operate on the 802.11a link.

Background scanning is enabled on a global basis on the associated controller of the access point. Latency might increase for voice calls when they are switched to a new channel.

In the EMEA regulatory domain, locating neighbors on other channels might take longer given DFS requirements.

Related Topics

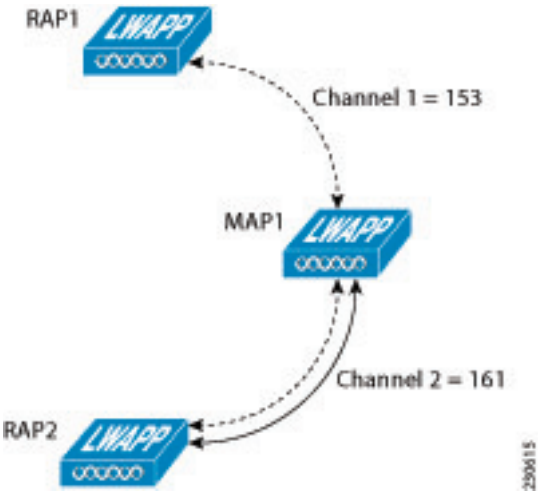
Mesh Network Background Scanning Scenarios, on page 45
Enable Mesh Network Background Scanning on Controllers, on page 46

Mesh Network Background Scanning Scenarios

A few scenarios are provided below to better illustrate how background scanning operates.

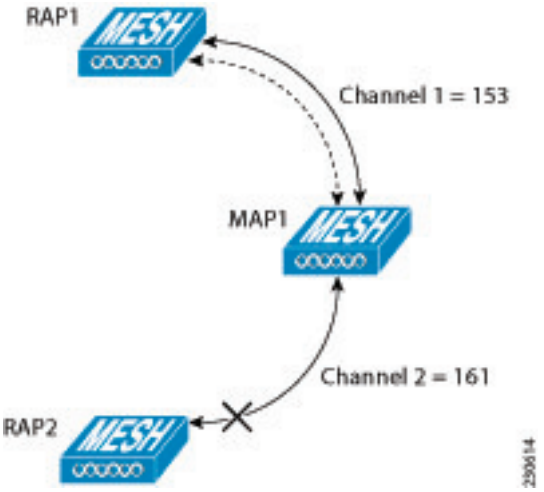
In the following figure, when the mesh access point (MAP1) initially comes up, it is aware of both root access points (RAP1 and RAP2) as possible parents. It chooses RAP2 as its parent because the route through RAP2 is better in terms of hops, SNR, and so on. After the link is established, background scanning (once enabled) continuously monitors all channels in search of a more optimal path and parent. RAP2 continues to act as parent for MAP1 and communicates on channel 2 until either the link goes down or a more optimal path is located on another channel.

Figure 6: Mesh Access Point (MAP1) Selects a Parent



In the following figure230614, the link between MAP1 and RAP2 is lost. Data from ongoing background scanning identifies RAP1 and channel 1 as the next best parent and communication path for MAP1 so that link is established immediately without the need for additional scanning after the link to RAP2 goes down.

Figure 7: Background Scanning Identifies a New Parent



Related Topics

Enable Mesh Network Background Scanning on Controllers, on page 46

Enable Mesh Network Background Scanning on Controllers

To enable background scanning on an AP1510 RAP or MAP:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click an IP address of the applicable controller.

Step 3 Choose **Mesh** > **Mesh Settings** from the left sidebar menu.

Step 4 Select the **Background Scanning** check box to enable background scanning or unselect it to disable the feature. The default value is disabled.

Step 5 This feature eliminates the time consuming task of finding a parent across channels by scanning all the channels. The off-channel procedure transmits broadcast packets on selected channels (at a periodicity of 3 seconds, with a maximum of 50 milliseconds per off-channel) and receives packets from all 'reachable' neighbors. This keeps the child MAP updated with neighbor information across channels enabling it to 'switch' to a new neighbor and use it as a parent for the uplink. The 'switch' need not be triggered from parent loss detection, but on identifying a better parent while the child MAP still has its current parent uplink active.

Step 6 Click **Save**.

Related Topics

Mesh Network Background Scanning Scenarios, on page 45

Configure Controller QoS Profiles

To make modifications to the quality of service profiles:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type> Wireless Controller**.

Step 2 Click an IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > QoS Profiles**. The following parameters appear:

- Bronze—For Background
- Gold—For Video Applications
- Platinum—For Voice Applications
- Silver—For Best Effort

Step 4 Click the applicable profile to view or edit profile parameters.

Step 5 Click **Save**.

Related Topics

Change Controller General System Properties from the Network Devices Table, on page 19

Information About Internal DHCP Server

Cisco Controllers have built-in DHCP (Dynamic Host Configuration Protocol) relay agents. However, when you desire network segments that do not have a separate DHCP server, the controllers can have built-in DHCP scopes that assign IP addresses and subnet masks to wireless client. Typically, one controller can have one or more DHCP scopes that each provide a range of IP addresses.

Note This feature is applicable for Cisco Mobility Express Release 8.3 and later.

Viewing Current DHCP Scopes

To view current DHCP (Dynamic Host Configuration Protocol) scopes, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the Device Name of the applicable controller.

Step 3 From the left sidebar menu, choose **System** > **DHCP Scopes**. The following parameters appear:

- Scope Name
- Pool Address
- Lease Time
- Pool Usage. This is displayed only for Cisco Mobility Express DHCP scopes.

Configuring DHCP Scopes

To add a new DHCP Scope, follow these steps.

Procedure

	Command or Action	Purpose
Step 1	Choose **Configuration** > **Network** > **Network Devices** > **Device Type** > **Wireless Controller**.	
Step 2	Click the Device Name of the applicable controller.	
Step 3	From the left sidebar menu, choose **System** > **DHCP Scopes**.	
Step 4	From the **Select a command** drop-down list, choose **Add DHCP Scope** to add a new DHCP scope, and click **Go**.	
Step 5	In the **Scope Name** text box, enter a name for the new DHCP scope.	
Step 6	In the **VLAN-ID** text box, enter the VLAN ID.	
Step 7	In the **Lease Time** text box, enter the amount of time (from 0 to 65,536 seconds) that an IP address is granted to a client.	
Step 8	In the **Network** text box, enter the network served by this DHCP scope. This IP address is used by the management	

	Command or Action	Purpose
	interface with Netmask applied, as configured on the Interfaces page.	
Step 9	In the **Netmask** text box, enter the subnet mask assigned to all wireless clients.	
Step 10	In the **Pool Start Address** text box, enter the starting IP address in the range assigned to the clients. This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.	
Step 11	In the **Pool End Address** text box, enter the ending IP address in the range assigned to the clients. This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.	
Step 12	In the **Default Gateway** text box, enter the IP address of the optional gateway.	
Step 13	In the **DNS Domain Name** text box, enter the optional DNS name of this DHCP scope for use with one or more DNS servers.	
Step 14	In the **DNS Servers** text box, enter the IP address of the optional DNS server. Each DNS server must be able to update a client's DNS entry to match the IP address assigned by this DHCP scope.	
Step 15	Click **Save**.	

Deleting DHCP Scopes

Note To delete a DHCP scope, you must first disable it's Admin status.

Procedure

	Command or Action	Purpose
Step 1	Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.	
Step 2	Click the Device Name of the applicable controller.	
Step 3	From the left sidebar menu, choose **System** > **DHCP Scopes**.	
Step 4	Select the check box of the DHCP Scope that you want to delete.	

	Command or Action	Purpose
Step 5	From the Select a command drop-down list, choose **Delete DHCP Scopes**, click **Go**.	

Exporting DHCP Scope Details

Procedure

	Command or Action	Purpose
Step 1	Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.	
Step 2	Click the Device Name of the applicable controller.	
Step 3	From the left sidebar menu, choose **System** > **DHCP Scopes**.	
Step 4	From the Select a command drop-down list, choose **DHCPLeases**, click **Go**.	
Step 5	Check the check box next to Mac Address, and Click **Export** to export the DHCP scope details as a csv file.	

View a Controller's Local Network Templates Used for Controller User Authentication

To view current local net user roles on a controller, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the Device Name of the applicable controller.

Step 3 From the left sidebar menu, choose **System** > **User Roles**.

The Local Net User Role parameters appear.

Step 4 Click a Template Name to view the User Role details.

Related Topics

Configure a Controller's Local Network Templates Used for Controller User Authentication , on page 51

Configure a Controller's Local Network Templates Used for Controller User Authentication

To add a new local net user role to a controller:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type> Wireless Controller**.

Step 2 Click the Device Name of the applicable controller.

Step 3 From the left sidebar menu, choose **System > User Roles**.

Step 4 From the Select a command drop-down list, choose **Add User Role**.

Step 5 Select a template from the Select a template to apply to this controller drop-down list.

Step 6 Click **Apply**.

Related Topics

View a Controller's Local Network Templates Used for Controller User Authentication, on page 50
Change Controller General System Properties from the Network Devices Table, on page 19

Configure a Controller Username and Password for APs Connecting to the Controller

The AP Username Password page enables you to set a global password that all access points inherit as they join a controller. When you are adding an access point, you can also choose to accept this global username and password or override it on a per-access point basis.

Also in controller software release 5.0, after an access point joins the controller, the access point enables console port security and you are prompted for your username and password whenever you log into the access point console port. When you log in, you are in non-privileged mode and you must enter the enable password to use the privileged mode.

To establish a global username and password, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type> Wireless Controller**.

Step 2 Click the Device Name of a controller with a Release 5.0 or later.

Step 3 From the left sidebar menu, choose **System > AP Username Password**.

Step 4 Enter the username and password that you want to be inherited by all access points that join the controller.

For Cisco IOS access points, you must also enter and confirm an enable password.

Step 5 Click **Save**.

Configure CDP on a Controller

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices.

CDP is enabled on the Ethernet and radio ports of a bridge by default.

Global Interface CDP configuration is applied to only the APs with CDP enabled at AP level.

To configure a Global CDP, perform the following steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type> Wireless Controller**.

Step 2 Click the Device Name of the desired controller.

Step 3 From the left sidebar menu, choose **System > Global CDP Configuration** from the left sidebar menu. The Global CDP Configuration page appears.

Step 4 Configure the required fields in the Global CDP Configuration page. In the Global CDP group box, configure the following parameters:

- CDP on controller—Choose enable or disable CDP on the controller. This configuration cannot be applied on WiSM2 controllers.
- Global CDP on APs—Choose to enable or disable CDP on the access points.
- Refresh-time Interval (seconds)—In the Refresh Time Interval field, enter the time in seconds at which CDP messages are generated. The default is 60.
- Holdtime (seconds)—Enter the time in seconds before the CDP neighbor entry expires. The default is 180.
- CDP Advertisement Version—Enter which version of the CDP protocol to use. The default is v1.

Step 5 In the CDP for Ethernet Interfaces group box, select the slots of Ethernet interfaces for which you want to enable CDP.

CDP for Ethernet Interfaces fields are supported for Controller Release 7.0.110.2 and later.

Step 6 In the CDP for Radio Interfaces group box, select the slots of Radio interfaces for which you want to enable CDP.

CDP for Radio Interfaces fields are supported for Controller Release 7.0.110.2 and later.

Step 7 Click **Save**.

Related Topics

Change Controller General System Properties from the Network Devices Table, on page 19

Configure 802.1X Authentication for Controllers

You can configure 802.1X authentication between lightweight access points and the switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC

provisioning. You can set global authentication settings that all access points inherit as they join the controller. This includes all access points that are currently joined to the controller and any that join in the future.

If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point.

To enable global supplicant credentials, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type> Wireless Controller**.

Step 2 Click the Device Name of the desired controller.

Step 3 From the left sidebar menu, choose **System > AP 802.1X Supplicant Credentials**.

Step 4 Select the **Global Supplicant Credentials** check box.

Step 5 Enter the supplicant username.

Step 6 Enter and confirm the applicable password.

Step 7 Select the **Supplicant EAP Type** from the dropdown menu.

Note Applicable for controllers and MEs with versions 8.7 onwards.

Related Topics

Change Controller General System Properties from the Network Devices Table, on page 19
Configure a Device's 802.11 Parameters , on page 113

Configure 802.1X Authentication for Controllers

You can configure 802.1X authentication between lightweight access points and the switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning. You can set global authentication settings that all access points inherit as they join the controller. This includes all access points that are currently joined to the controller and any that join in the future.

If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point.

To enable global supplicant credentials, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type> Wireless Controller**.

Step 2 Click the Device Name of the desired controller.

Step 3 From the left sidebar menu, choose **System > AP 802.1X Supplicant Credentials**.

Step 4 Select the **Global Supplicant Credentials** check box.

Step 5 Enter the supplicant username.

Step 6 Enter and confirm the applicable password.

Step 7 Select the **Supplicant EAP Type** from the dropdown menu.

Note Applicable for controllers and MEs with versions 8.7 onwards.

Related Topics

Change Controller General System Properties from the Network Devices Table, on page 19
Configure a Device's 802.11 Parameters , on page 113

Configure DHCP on a Controller

To configure DHCP (Dynamic Host Configuration Protocol) information for a controller:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type> Wireless Controller**.

Step 2 Click the Device Name of the desired controller.

Step 3 From the left sidebar menu, choose **System > DHCP**.

Step 4 Add or modify the following parameters:

- DHCP Option 82 Remote Id Field Format—Choose **AP-MAC, AP-MAC-SSID, AP-ETHMAC, or AP-NAME-SSID** from the drop-down list.

To set the format for RemoteID field in DHCP option 82If Ap-Mac is selected, then set the RemoteID format as *AP-Mac*. If Ap-Mac-ssid is selected, then set the RemoteID format as *AP-Mac:SSID*.

- DHCP Proxy—Select the check box to enable DHCP by proxy.

When DHCP proxy is enabled on the controller, the controller unicasts DHCP requests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the WLAN or the WLAN itself.

Step 5 Enter the DHCP Timeout in seconds after which the DHCP request times out. The default setting is 5. Allowed values range from 5 to 120 seconds. DHCP Timeout is applicable for Controller Release 7.0.114.74 and later.

Step 6 Click **Save**.

Once saved, you can click **Audit** to perform an audit on this controller.

Related Topics

Change Controller General System Properties from the Network Devices Table, on page 19

Configure Multicast Mode and IGMP Snooping on a Controller

Prime Infrastructure provides an option to configure IGMP (Internet Group Management Protocol) snooping and timeout values on the controller.

IGMP

To configure multicast mode and IGMP snooping for a controller:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the Device Name of the desired controller.

Step 3 From the left sidebar menu, choose **System** > **Multicast**.

Step 4 From the Ethernet Multicast Support drop-down list, choose the applicable Ethernet multicast support (Unicast or Multicast).

Step 5 If Multicast is selected, enter the multicast group IP address.

Step 6 Select the Global Multicast Mode check box to make the multicast mode available globally.

IGMP Snooping and timeout can be set only if Ethernet Multicast mode is Enabled. Select to enable IGMP Snooping.

Step 7 Choose **Enable** from the Multicast Mobility Mode drop-down list to change the IGMP snooping status or to set the IGMP timeout. When IGMP snooping is enabled, the controller gathers IGMP reports from the clients and then sends each access point a list of the clients listening to any multicast group. The access point then forwards the multicast packets only to those clients.

The timeout interval has a range of 3 to 300 and a default value of 60. When the timeout expires, the controller sends a query to all WLANs. Those clients which are listening in the multicast group then send a packet back to the controller.

Step 8 If you enabled the Multicast Mobility Mode, enter the mobility group multicast address.

Step 9 Select the **Multicast Direct** check box to enable videos to be streamed over a wireless network.

Step 10 Choose **Enable** from the Multicast Mobility Mode drop-down list to change MLD configuration.

Step 11 Select the **Enable MLD Snooping** check box to enable IPv6 MLD snooping. If you have selected this check box, configure the following parameters:

- MLD Timeout—Enter the MLD timeout value in seconds. The timeout has a range of 3 to 7200 and a default value of 60.
- MLD Query Interval—Enter the MLD query interval timeout value in seconds. The interval has a range of 15 to 2400 and a default value of 20.

Internet Group Management Protocol (IGMP) snooping enables you to limit the flooding of multicast traffic for IPv4. For IPv6, Multicast Listener Discovery (MLD) snooping is used.

Step 12 Configure the Session Banner information, which is the error information sent to the client if the client is denied or dropped from a Media Stream.

Step 13 Click **Save**.

Once saved, you can click **Audit** to perform an audit on this controller.

Related Topics

Change Controller General System Properties from the Network Devices Table, on page 19

Configure a Controller 's Advanced Timers to Reduce Failure Detection Time

Advanced timer configuration for FlexConnect and local mode is available for the controller on Prime Infrastructure.

This feature is only supported on Release 6.0 controllers and later.

To configure the advanced timers, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices** , then from the Devices Groups menu on the left, select **Device Type> Wireless Controller**.

Step 2 Choose the controller for which you want to set timer configuration.

Step 3 From the left sidebar menu, choose **System > AP Timers**.

Step 4 In the AP Timers page, click the applicable Access Point Mode link: Local Mode or FlexConnect Mode.

Step 5 Configure the necessary parameters in the Local Mode AP Timer Settings page or in the FlexConnect Mode AP Timer Settings page accordingly.

- AP timer settings for Local Mode—To reduce the failure detection time, you can configure the fast heartbeat interval (between the controller and the access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller. You can then enter a value between 10 and 15 seconds.
- AP timer settings for FlexConnect—Once selected, you can configure the FlexConnect timeout value. Select the **AP Primary Discovery Timeout** check box to enable the timeout value. Enter a value between 30 and 3600 seconds. 5500 series controllers accept access point fast heartbeat timer values in the range of 1-10.

Step 6 Click **Save**.

Related Topics

Create WLANs on a Controller, on page 56

Create WLANs on a Controller

Because controllers can support 512 WLAN configurations, Prime Infrastructure provides an effective way to enable or disable multiple WLANs at a specified time for a given controller.

To view a summary of the wireless local access networks (WLANs) that you have configured on your network, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type** > **Wireless Controller**.

Step 2 Click the Device Name of the applicable controller.

Step 3 From the left sidebar menu, choose **WLANs** > **WLAN Configuration**.

Step 4 Configure the required fields in the Configure WLAN Summary page.

Related Topics

View the WLANs Configured on a Controller, on page 57
Add Security Policies to WLANs on a Controller, on page 57
Configure Mobile Concierge (802.11u) on a Controller, on page 58
Add a WLAN to a Controller, on page 61
Delete a WLAN from a Controller, on page 61

Change the Admin Status of a Controller's WLANs, on page 61
View a Controller WLAN's Mobility Anchors, on page 62
Configure a Controller's WLAN AP Groups, on page 65

View the WLANs Configured on a Controller

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the Device Name of the wireless controller whose WLAN configurations you want to see.

Step 3 Click the **Configuration** tab.

Step 4 Under **Features**, choose**WLANs** > **WLAN Configuration**. The WLAN Configuration summary page appears, displaying the list of WLANs currently configured on the controller, including each:

- WLAN ID
- The name of the WLAN configuration profile
- WLAN SSID
- The names of any active security policies
- The WLAN current administrative status (enabled or disabled)
- A link to the list of all currently scheduled WLAN configuration tasks

Step 5 To view WLAN configuration details, click the **WLAN ID**. The WLAN Configuration details page appears.

Step 6 Use the tabs (General, Security, QoS, and Advanced) to view or edit parameters for the WLAN. Whenever you change a parameter, click **Save**.

Related Topics

Add Security Policies to WLANs on a Controller, on page 57
Configure Mobile Concierge (802.11u) on a Controller, on page 58
Add a WLAN to a Controller, on page 61
Delete a WLAN from a Controller, on page 61
Change the Admin Status of a Controller's WLANs, on page 61
View a Controller WLAN's Mobility Anchors, on page 62

Add Security Policies to WLANs on a Controller

Step 1 Navigate to WLAN Configuration details page as described in View the WLANs Configured on a Controller.

Step 2 Click **Policy Mappings** tab.

Step 3 Click **Add Row**.

Step 4 Select a policy name that you want to map to the WLAN, from the drop-down list.

Step 5 Enter the priority. The priority ranges from 1 to 16.

Two policies cannot have the same priority.

Step 6 Click **Save**.

If you want to delete a policy, select the check box corresponding to the policy that you want to delete and click Delete.

Related Topics

View the WLANs Configured on a Controller, on page 57
Configure Mobile Concierge (802.11u) on a Controller, on page 58
Add a WLAN to a Controller, on page 61
Delete a WLAN from a Controller, on page 61
Change the Admin Status of a Controller's WLANs, on page 61
View a Controller WLAN's Mobility Anchors, on page 62

Configure Mobile Concierge (802.11u) on a Controller

Cisco Mobile Concierge is a solution that enables 802.1X-capable clients to interwork with external networks without pre-authorization. Mobile Concierge provides service availability information to clients that can help them to associate to available networks more quickly, easily, and securely.

The services offered by the network can be broadly classified into two protocols:

- 802.11u MSAP
- 802.11u HotSpot 2.0

The following guidelines and limitations apply to Mobile Concierge:

- Mobile Concierge is not supported on FlexConnect Access Points.
- 802.11u configuration upload is not supported. If you perform a configuration upgrade and upload a configuration on the controller, the HotSpot configuration on the WLANs is lost.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type** > **Wireless Controller**.

Step 2 Click the Device Name of the wireless controller on which you want to configure Mobile Concierge.

Step 3 Click the **Configuration** tab.

Step 4 Under **Features**, choose **WLANs** > **WLAN Configuration>** . The WLAN Configuration summary page appears, displaying the list of WLANs currently configured on the controller,

Step 5 Click the WLAN ID of the WLAN on which you want to configure Mobile Concierge.

Step 6 Click the **Hot Spot** tab.

Step 7 Click the **802.11u Configuration** sub-tab and complete the fields as follows:

a) Select the **802.11u Status** check box to enable 802.11u on the WLAN.

b) Select the **Internet Access** check box to enable this WLAN to provide Internet services.

c) From the **Network Type** drop-down list, choose the appropriate description for the 802.11u service you want to configure on this WLAN. The following options are available:

- **Private Network**
- **Private Network with Guest Access**
- **Chargeable Public Network**
- **Free Public Network**
- **Emergency Services Only Network**

- **Personal Device Network**
- **Test or Experimental**
- **Wildcard**

d) Choose the authentication type that you want to configure for the 802.11u parameters on this network:

- Not configured
- Acceptance of Terms and Conditions
- Online Enrollment
- DNS Redirection
- HTTP/HTTPS Redirection

e) In the **HESSID** field, enter the Homogeneous Extended Service Set Identifier value. The HESSID is a 6-octet MAC address that identifies the homogeneous ESS.

f) In the **IPv4 Address Type** field, choose the method of assigning IPv4 addresses:

- **Not Available**
- **Public**
- **Port Restricted**
- **Single NAT Private**
- **Double NAT Private**
- **Port Restricted and Single NAT Private**
- **Port Restricted and Double NAT Private**
- **Unknown**

g) In the **IPv6 Address Type** field, choose the method of assigning IPv6 addresses:

- **Not Available**
- **Available**
- **Unknown**

Step 8 Click the **Others** sub-tab and complete the fields as follows:

a) In the OUI List group box, click **Add Row** and enter the following details:

- OUI name
- Is Beacon
- OUI Index

Click **Save** to add the OUI (Organizationally Unique Identifier) entry to this WLAN.

b) In the Domain List group box, click **Add Row** and enter the following details:

- Domain Name—The domain name operating in the 802.11 access network.
- Domain Index—Choose the domain index from the drop-down list.

Click **Save** to add the domain entry to this WLAN.

c) In the Cellular section, click **Add Row** and enter the following details:

- Country Code—The 3-character cellular country code.
- Network Code—The 3-character cellular network code.

Click **Save** to add the cellular entry to this WLAN.

Step 9 Click the **Realm** sub-tab and complete the fields as follows:

a) Click **Add Row** and enter the realm name.
b) Click **Save** to add the realm entry to this WLAN.

Step 10 Click the **Service Advertisements** sub-tab and complete the fields as follows:

a) Select the **MSAP Enable** check box to enable service advertisements.
b) If you enable MSAP, enter the server index for this WLAN. The server index field uniquely identifies an MSAP server instance serving a venue that is reachable through the BSSID.

MSAP (Mobility Services Advertisement Protocol) is designed to be used primarily by mobile devices that are configured with a set of policies for establishing network services. These services are available for devices that offer higher-layer services, or network services that are enabled through service providers. Service advertisements use MSAP to provide services to mobile devices prior to association to a Wi-Fi access network. This information is conveyed in a service advertisement. A single-mode or dual-mode mobile device queries the network for service advertisements before association. The device's network discovery and the selection function may use the service advertisements in its decision to join the network.

Step 11 Click the **Hotspot 2.0** sub-tab and complete the fields as follows:

a) Choose the **Enable** option from the HotSpot2 Enable drop-down list.
b) In the WAM Metrics group box, specify the following:

- WAN Link Status—The link status. The valid range is 1 to 3.
- WAN SIM Link Status—The symmetric link status. For example, you can configure the uplink and downlink to have different speeds or same speeds.
- Up Link Speed—The uplink speed. The maximum value is 4,194,304 kbps.
- Down Link Speed—The downlink speed. The maximum value is 4,194,304 kbps.

c) In the Operator Name List, click **Add Row** and enter the following details:

- Operator Name—Specify the name of the 802.11 operator.
- Operator Index—Select an operator index. The range is from 1 to 32.
- Language Code—An ISO-14962-1997 encoded string defining the language. This string is a three character language code.

Click **Save** to add the operator to the list.

d) In the Port Config List, click **Add Row** and enter the following details:

- IP Protocol—The IP protocol that you want to enable. The following options are ESP, FTP, ICMP, and IKEV2.
- Port No—The port number that is enabled on this WLAN.
- Status—The status of the port.

Click **Save** to add the port configuration to the list.

Step 12 Click **Save** to save the Mobile Concierge configuration.

Related Topics

View the WLANs Configured on a Controller, on page 57
Add a WLAN to a Controller, on page 61
Delete a WLAN from a Controller, on page 61
Change the Admin Status of a Controller's WLANs, on page 61
Add Security Policies to WLANs on a Controller, on page 57
View a Controller WLAN's Mobility Anchors, on page 62

Add a WLAN to a Controller

Step 1 Choose **Configuration** > **Template** > **Features & Technologies** > **Controller** > **WLANsWLAN Configuration**.

Step 2 Hover your mouse cursor over the tool tip next to the template type and click **New**.

Step 3 Complete the required fields in the General, Security, QoS, Advanced, HotSpot, Policy Mappings tabs, and then click **Save as New Template**.

Step 4 Proceed to deploy the template by click **Deploy**.

Related Topics

View the WLANs Configured on a Controller, on page 57
Configure Mobile Concierge (802.11u) on a Controller, on page 58
Delete a WLAN from a Controller, on page 61
Change the Admin Status of a Controller's WLANs, on page 61
Add Security Policies to WLANs on a Controller, on page 57
View a Controller WLAN's Mobility Anchors, on page 62
Configure a Controller's WLAN AP Groups, on page 65

Delete a WLAN from a Controller

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type** > **Wireless Controller**.

Step 2 Click the Device Name of the appropriate controller.

Step 3 From the left sidebar menu, choose **WLANs** > **WLAN Configuration**.

Step 4 Select the check boxes of the WLANs that you want to delete.

Step 5 Choose **Select a command** > **Delete a WLAN** > **Go**.

Step 6 Click **OK** to confirm the deletion.

Related Topics

View the WLANs Configured on a Controller, on page 57
Configure Mobile Concierge (802.11u) on a Controller, on page 58
Add a WLAN to a Controller, on page 61
Change the Admin Status of a Controller's WLANs, on page 61
Add Security Policies to WLANs on a Controller, on page 57
View a Controller WLAN's Mobility Anchors, on page 62

Change the Admin Status of a Controller's WLANs

Prime Infrastructure lets you change the status of more than one WLAN at a time on any given controller. You can select multiple WLANs and select the date and time for that status change to take place.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type** > **Wireless Controller**.

Step 2 Click the Device Name of the appropriate controller.

Step 3 From the left sidebar menu, choose **WLANs** > **WLAN Configuration**.

Step 4 Select the check boxes of the WLANs that you want to schedule for a status change.

Step 5 From the Select a command drop-down list, choose **Schedule Status** to open the WLAN Schedule Task Detail page.

The selected WLANs are listed at the top of the page.

Step 6 Enter a Scheduled Task Name to identify this status change schedule.

Step 7 Choose the new Admin Status (Enabled or Disabled) from the drop-down list.

Step 8 Choose the schedule time using the hours and minutes drop-down lists.

Step 9 Click the calendar icon to choose a schedule date or enter the date in the text box (MM/DD/YYYY).

Step 10 Select the appropriate Recurrence radio button to determine the frequency of the status change (Daily, Weekly, or No Recurrence).

Step 11 Click **Submit** to initiate the status change schedule.

Related Topics

View the WLANs Configured on a Controller, on page 57
Configure Mobile Concierge (802.11u) on a Controller, on page 58
Add a WLAN to a Controller, on page 61
Delete a WLAN from a Controller, on page 61
Add Security Policies to WLANs on a Controller, on page 57
View a Controller WLAN's Mobility Anchors, on page 62

View a Controller WLAN's Mobility Anchors

Mobility anchors are controllers defined as anchors for WLANs. Clients (that is, any 802.11 mobile station, such as a laptop) are always attached to one of the anchors.

You can use mobility anchors to restrict a WLAN to a single subnet, regardless of the client's network entry point. Users can access a public or guest WLAN throughout the enterprise but will still be restricted to a specific subnet. You can also use guest WLANs to provide geographical load balancing, as WLANs can represent a particular section of a building (such as a lobby, restaurant, and so on).

When a client first associates to a controller of a mobility group that has been preconfigured as a mobility anchor for a WLAN, the client associates to the controller locally, and a local session is created for the client. Clients can be anchored only to preconfigured anchor controllers of the WLAN. For a given WLAN, you should configure the same set of anchor controllers on all controllers in the mobility group.

When a client first associates to a controller of a mobility group that has not been configured as a mobility anchor for a WLAN, the client associates to the controller locally, a local session is created for the client, and the controller is announced to the other controllers in the same mobility group. If the announcement is not answered, the controller contacts one of the anchor controllers configured for the WLAN and creates a foreign session for the client on the local switch. Packets from the client are encapsulated and delivered to the wired network. Packets to the client are received by the anchor controller and forwarded to the foreign controller through a mobility tunnel using EtherIP. The foreign controller encapsulates the packets and forwards them to the client.

A 2000 series controller cannot be designated as an anchor for a WLAN. However, a WLAN created on a 2000 series controllers can have a 4100 series controller or a 4400 series controller as its anchor.

The L2TP Layer 3 security policies are unavailable for WLANs configured with a mobility anchor.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the Device Name of the appropriate controller.

Step 3 From the left sidebar menu, choose **WLANs** > **WLAN Configuration**.

Step 4 Click a WLAN ID to view the parameters for a specific WLAN.

Step 5 Click the **Advanced** tab.

Step 6 Click the **Mobility Anchors** link. Prime Infrastructure displays the IP address and current status (for example, reachable) for each anchor.

Related Topics

View the WLANs Configured on a Controller, on page 57
Configure Mobile Concierge (802.11u) on a Controller, on page 58
Add a WLAN to a Controller, on page 61
Delete a WLAN from a Controller, on page 61
Change the Admin Status of a Controller's WLANs, on page 61
Add Security Policies to WLANs on a Controller, on page 57

Configuring 802.11r Fast Transition

An 802.11r-enabled WLAN provides faster and better roaming experience for wireless client devices. However, legacy devices that do not recognize fast transition (FT) authentication key-management (AKM) in a robust secure network information exchange (in beacons and probe responses) cannot join the 802.11r-enabled WLAN.

Procedure

	Command or Action	Purpose
Step 1	Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type** > **Wireless Controller** to view all the wireless controllers.	
Step 2	Click the name of the corresponding controller.	
Step 3	From the left sidebar menu, choose **WLANs** > **WLAN Configuration**to access the WLAN Configuration page.	
Step 4	Click the corresponding WLAN ID to view the parameters for that specific WLAN.	
Step 5	Choose **Security** > **Layer 2**tab.	
Step 6	From the **Layer 2 Security** drop-down list, choose WPA+WPA2.	The Authentication Key Management parameters for Fast Transition are displayed

	Command or Action	Purpose
Step 7	Check or uncheck the Fast Transition check box to enable or disable Fast Transition. Fast Transition is enabled by default when you create a new WLAN, from Cisco WLC Release 8.3onwards. However, the existing WLANs will retain the current configuration when Cisco WLC upgrades to Release 8.3 from an earlier release.	
Step 8	Check or uncheck the **Over the DS** check box to enable or disable Fast Transition over a distributed system. This option is available only if you enable Fast Transition or if Fast Transition is adaptive.	
Step 9	In the **Reassociation Timeout** text box, enter the number of seconds after which the reassociation attempt of a client to an AP should time out. The valid range is 1 to 100 seconds.	This option is available only if you enable Fast Transition.
Step 10	Under **Authentication Key Management**, choose **FT 802.1X** or **FT PSK**. Check or uncheck corresponding check boxes to enable or disable the keys. If you check the FT PSK check box, from the **PSK Format** drop-down list, choose **ASCII** or **HEX** and enter the key value.	When Fast Transition adaptive is enabled, you can use only 802.1X and PSK.
Step 11	Click **Save** to save your settings.	

Configure Fastlane QoS

The Fastlane QoS feature provides better Quality of Service (QoS) treatment for Apple clients, when compared to other wireless clients. This feature is disabled by default.

Note Enable or disable this feature only during a maintenance window, when not many clients are connected. This is because there will be a disruption in service when all the WLANs and the network are disabled and enabled again.

Procedure

	Command or Action	Purpose
Step 1	Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type** > **Wireless Controller**.	
Step 2	Click the name of the corresponding controller.	
Step 3	From the left sidebar menu, choose **WLANs** > **WLAN Configuration**.	
Step 4	Click the corresponding WLAN ID to view the parameters for that specific WLAN.	

	Command or Action	Purpose
Step 5	Click the**QoS** tab.	
Step 6	Check the **Fastlane** check box to enable Fastlane QoS.	
Step 7	Click **Save** to save your settings.	

Disable Fastlane QoS

Note Fastlane must be disabled on all the WLANs before disabling Fastlane QoS.

Procedure

	Command or Action	Purpose
Step 1	Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type** > **Wireless Controller**.	
Step 2	Click **Device Name** of the appropriate controller.	
Step 3	From the left sidebar menu, choose **WLANs** > **WLAN Configuration**.	
Step 4	From the **Select a Command** drop-down list, choose **Disable Fastlane**.	
Step 5	Click **Save** to save your settings.	

Configure a Controller's WLAN AP Groups

Site-specific VLANs or AP (access point) groups allow you to segment WLANs into different broadcast domains. This will allow you to minimize the total number of broadcast domains, which permits more effective load balancing and bandwidth allocation.

Step 1 Choose **Configuration > Network > Network Devices**, then select **Device Type > Wireless Controller**.

Step 2 Click the Device Name of the appropriate controller.

Step 3 From the left sidebar menu, choose **WLAN > AP Groups**. The AP groups summary page displays.

This page displays a summary of the AP groups configured on your network.

From here you can remove or view details of an AP group.

Step 4 Click the AP group name on the Access Points tab to view or edit its access point(s).

Step 5 Click the **WLAN Profiles** tab to view, edit, add, or delete WLAN profiles.

Related Topics

Create Controller WLAN AP Groups, on page 66
Delete Controller WLAN AP Groups, on page 67
Create WLANs on a Controller, on page 56
Audit Controller WLAN AP Groups to Locate Configuration Differences , on page 68

Create Controller WLAN AP Groups

Use the AP Groups detail page to add AP (access point) groups. Note that if the target controller is earlier than version 5.2, *AP Groups* are called *AP Group VLANs* .

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type > Wireless Controller**.

Step 2 Click the Device Name of the appropriate controller.

Step 3 From the left sidebar menu, choose **WLAN** > **AP Groups**.

Step 4 Choose **Select a command** > **Add AP Groups** > **Go**. The AP Groups details page displays.

Step 5 Create a new AP group, as follows:

a) Enter a name for the AP group.
b) Enter a description for the new AP group (this group description is optional).

Step 6 Add access points to the new AP group, as follows:

a) Click the **Access Points** tab.
b) Click **Add**. The Access Point page displays a list of available access points.
c) Select the check boxes of the access points you want to add.
d) Click **Select**.

Step 7 Add a WLAN profile, as follows:

a) Click the **WLAN Profiles** tab.
b) Click **Add**.

To display all available WLAN profile names, delete the current WLAN profile name from the text box. When the current WLAN profile name is deleted from the text box, all available WLAN profiles appear in the drop-down list.

Each access point is limited to 16 WLAN profiles. Each access point broadcasts all WLAN profiles unless the WLAN override feature is enabled. The WLAN override feature allows you to disable any of the 16 WLAN profiles per access point.

The WLAN override feature applies only to older controllers that do not support the 512 WLAN feature (can support up to 512 WLAN profiles).

c) Type a WLAN profile name or choose one from the WLAN Profile Name drop-down list.
d) Enter an interface/interface group or choose one from the Interface/Interface Group drop-down list.

To display all available interfaces, delete the current interface in the Interface text box. When the current interface is deleted from the Interface text box, all available interfaces appear in the drop-down list.

e) Select the **NAC Override** check box, if applicable. NAC override is disabled by default.
f) Specify the policy configuration parameters by clicking the **Add/Edit** link.

- Policy Name—Name of the policy.

- Policy Priority—Configure policy priority between 1 and 16. No two policies can have same priority.

Only 16 Policy mappings are allowed per WLAN. Selected policy template for the mapping will be applied first if it does not exist on the controller.

g) When access points and WLAN profiles are added, click **Save**.

Step 8 (Optional): Add an RF profile, as follows:

a) Click the **RF Profiles** tab:

b) Complete the fields as follows:

- 802.11a—Choose an RF profile for APs with 802.11a radios.
- 802.11b—Choose an RF profile for APs with 802.11b radios.

Step 9 Add Hyperlocation configuration parameters, as follows:

- Click the Location Settings tab and configure the following:
  - Hyperlocation— By enabling this option, all the APs associated to that controller which have the Hyperlocation module will be enabled.
  - Packet Detection RSSI Minimum—Adjust this value to filter out weak RSSI readings from location calculation.
  - Scan Count Threshold for Idle Client Detection—The maximum permissible count of the idle clients detected while scanning.
  - NTP Server IP Address—Enter the valid NTP server IP address.This IP address is used by all APs for time synchronization.

Step 10 When you are finished adding APs, WLAN profiles, and RF profiles to the new AP Group, click **Save**.

Changing the WLAN-interface mapping in an AP Group removes the local VLAN mapping for FlexConnect APs in this group. These mappings need to be reconfigured after applying this change.

Related Topics

Configure a Controller's WLAN AP Groups, on page 65
Delete Controller WLAN AP Groups, on page 67
Audit Controller WLAN AP Groups to Locate Configuration Differences , on page 68

Delete Controller WLAN AP Groups

Step 1 Choose **Configuration > Network > Network Devices**, then select **Device Type > Wireless Controller**.

Step 2 Click the Device Name of the appropriate controller.

Step 3 From the left sidebar menu, choose **WLAN > AP Groups**.

Step 4 Select the check box(es) of the AP Groups that you want to delete.

Step 5 Choose **Select a command > Delete AP Groups > Go**.

Step 6 Click **OK** to confirm the deletion.

Related Topics

Configure a Controller's WLAN AP Groups, on page 65

Create Controller WLAN AP Groups, on page 66
Audit Controller WLAN AP Groups to Locate Configuration Differences , on page 68

Audit Controller WLAN AP Groups to Locate Configuration Differences

It is possible for difference to occur between the values Prime Infrastructure has stored for an AP group and the actual values stored in the current controller and access points device configurations. Auditing the AP group will help you determine if this has occurred and resolve them.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type > Wireless Controller**.

Step 2 Click the Device Name of the appropriate controller.

Step 3 From the left sidebar menu, choose **WLAN > AP Groups**.

Step 4 Click the name of the access point group that you want to audit.

Step 5 Click **Audit.**

The **Audit** button is located at the bottom of the page, next to the **Save** and **Cancel** buttons

Related Topics

Create Controller WLAN AP Groups, on page 66
Delete Controller WLAN AP Groups, on page 67
Create WLANs on a Controller, on page 56

Information About Captive Portal Bypassing

A captive portal is a web page where users are redirected to when they connect to a network, which usually displays information about Terms of Service and also used for login Authentication WISPr is a draft protocol that enables users to roam between different wireless service providers. Some devices (for example, Apple iOS devices) have a mechanism using which they can determine if the device is connected to Internet, based on an HTTP WISPr request made to a designated URL. This mechanism is used for the device to automatically open a web browser when a direct connection to the Internet is not possible. This enables the user to provide his credentials to access the Internet. The actual authentication is done in the background every time the device connects to a new SSID.

The client device (Apple IOS device) sends a WISPr request to the controller, which checks for the user agent details and then triggers an HTTP request with a web authentication interception in the controller. After verification of the IOS version and the browser details provided by the user agent, the controller allows the client to bypass the captive portal settings and provides access to the Internet.

This HTTP request triggers a web authentication interception in the controller as any other page requests are performed by a wireless client. This interception leads to a web authentication process, which will be completed normally. If the web authentication is being used with any of the controller splash page features (URL provided by a configured RADIUS server), the splash page may never be displayed because the WISPr requests are made at very short intervals, and as soon as one of the queries is able to reach the designated server, any web redirection or splash page display process that is performed in the background is aborted, and the device

processes the page request, thus breaking the splash page functionality. For example, Apple introduced an iOS feature to facilitate network access when captive portals are present. This feature detects the presence of a captive portal by sending a web request on connecting to a wireless network. This request is directed to http://www.apple.com/library/test/success.html for Apple IOS version 6 and older, and to several possible target URLs for Apple IOS version 7 and later. If a response is received, then the Internet access is assumed to be available and no further interaction is required. If no response is received, then the Internet access is assumed to be blocked by the captive portal and Apple's Captive Network Assistant (CNA) auto-launches the pseudo-browser to request portal login in a controlled window. The CNA may break when redirecting to an ISE captive portal. The controller prevents this pseudo-browser from popping up.

You can now configure the controller to bypass WISPr detection process so the web authentication interception is only done when a user requests a web page leading to splash page load in user context, without the WISPr detection being performed in the background.

Configuring Captive Network Portal Bypass

Procedure

	Command or Action	Purpose
Step 1	Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type** > **Wireless Controller**.	
Step 2	Click a Device Name, then click the **Configuration** tab.	
Step 3	Choose **System** > **General - System** to access the General page.	
Step 4	From the **Captive Network Assistant** Bypass drop-down list, choose **Enable**.	

Configuring Captive Network Portal Bypass Per WLAN

Procedure

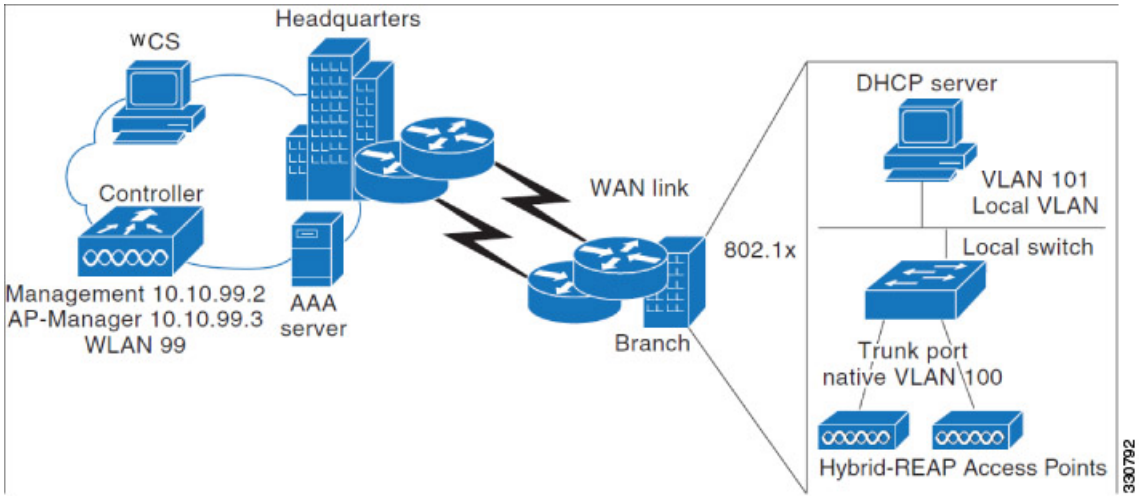
	Command or Action	Purpose
Step 1	Choose **Configuration** > **Network** > **Network Devices**, then select **Device Type** > **Wireless Controller**.	
Step 2	Click a Device Name.	
Step 3	Choose **WLANs** > **WLAN Configuration** from the left sidebar menu.	
Step 4	Click the **WLAN ID**.	
Step 5	Click the **Security** > **Layer 3** tab to modify the default security policy.	
Step 6	From the **Captive Network Assistant** Bypass drop-down list, choose **Enable**.	
Step 7	Click **Save**.	

Configure and Monitor APs Using FlexConnect

FlexConnect enables you to configure and control APs in a remote location from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The FlexConnect APs switch client data traffic and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller.

The following figure illustrates a typical FlexConnect deployment.

Figure 8: FlexConnect Deployment



Related Topics

Supported Devices for FlexConnect, on page 70
Prerequisites for Using FlexConnect, on page 71
How FlexConnect Performs Authentication, on page 71
FlexConnect Operation Modes: Connected and Standalone, on page 72
FlexConnect States, on page 72

Supported Devices for FlexConnect

FlexConnect is supported only on these components:

- 1130AG, 1240AG, 1142, and 1252 APs
- Cisco 2000, and 4400 series controllers,
- Catalyst 3750G Integrated Wireless LAN Controller Switch
- Cisco Wireless Services Module (WiSM)
- Controller Network Module for Integrated Services Routers

Related Topics

Prerequisites for Using FlexConnect, on page 71
How FlexConnect Performs Authentication, on page 71
FlexConnect Operation Modes: Connected and Standalone, on page 72
FlexConnect States, on page 72

Prerequisites for Using FlexConnect

Follow these guidelines when you configure FlexConnect:

- You can deploy FlexConnect with either a static IP address or a DHCP address. The DHCP server must be available locally and must be able to provide the IP address for the AP during bootup.
- The maximum transmission unit (MTU) must be at least 500 bytes.
- Round-trip latency must not exceed 300 milliseconds (ms) between the AP and the controller. If the 300 milliseconds round-trip latency cannot be achieved, configure the AP to perform local authentication.
- The controller can send multicast packets in the form of unicast or multicast packets to the AP. In FlexConnect mode, the AP can receive multicast packets only in unicast form.
- FlexConnect supports CCKM full authentication but not CCKM fast roaming.
- FlexConnect supports a 1-1 network address translation (NAT) configuration and port address translation (PAT) for all features except true multicast. Multicast is supported across NAT boundaries when configured using the Unicast option.
- VPN, IPsec, L2TP, PPTP, Fortress authentication, and Cranite authentication are supported for locally switched traffic if these security types are accessible locally at the AP.
- NAC out-of-band integration is supported only on WLANs configured for FlexConnect central switching. It is not supported for use on WLANs configured for FlexConnect local switching.
- For FlexConnect APs, the interface mapping at the controller for WLANs configured for FlexConnect local switching is inherited at the AP as the default VLAN tagging. This can be easily changed per SSID and per FlexConnect AP. Non-FlexConnect APs tunnel all traffic back to the controller, and VLAN tagging is dictated by each interface mapping of the WLAN
- VLAN is not enabled on the FlexConnect AP by default. When FlexConnect is enabled, the AP inherits the VLAN ID associated to the WLAN. This configuration is saved in the AP and received after the successful join response. By default, the native VLAN is 1. One native VLAN must be configured per FlexConnect AP in a VLAN-enabled domain. Otherwise, the AP cannot send and receive packets to and from the controller. When the client is assigned a VLAN from the RADIUS server, that VLAN is associated to the locally switched WLAN.

Related Topics

How FlexConnect Performs Authentication, on page 71

How FlexConnect Performs Authentication

A FlexConnect AP searches for a controller on booting up. The AP joins the controller, downloads the latest software image from the controller and configuration information, and initializes the radio. It saves the downloaded configuration in non-volatile memory for use in standalone mode.

A FlexConnect AP identifies the controller IP address in one of the following ways:

- If the AP has been assigned an IP address from a DHCP server, it discovers a controller through the regular CAPWAP discovery process [Layer 3 broadcast, over-the-air provisioning (OTAP), DNS, or DHCP option 43]. OTAP does not work when the AP is booting up for the first time.
- If the AP has been assigned a static IP address, it discovers a controller through any of the CAPWAP discovery process methods except DHCP option 43. If the AP is unable to discover a controller through Layer 3 broadcast or OTAP, we recommend DNS resolution. With DNS, any AP with a static IP address that knows of a DNS server can find at least one controller.
- If you want the AP to discover a controller from a remote network where CAPWAP discovery mechanisms are not available, you can use priming. This method enables you to specify (through the AP command-line interface) the controller to which the AP should connect.

Related Topics

Supported Devices for FlexConnect, on page 70
Prerequisites for Using FlexConnect, on page 71
FlexConnect Operation Modes: Connected and Standalone, on page 72
FlexConnect States, on page 72

FlexConnect Operation Modes: Connected and Standalone

The two modes of operation for FlexConnect APs are:

- Connected mode— In this mode the FlexConnect AP has CAPWAP connectivity with the controller.
- Standalone mode—In this mode the controller is unreachable and the FlexConnect AP enters standalone mode and authenticates clients by itself.

When a FlexConnect AP enters standalone mode:

-
  - All clients that are on centrally switched WLANs are disassociated.
  - For 802.1X or web-authentication WLANs, existing clients are not disassociated, but the FlexConnect AP stops sending beacons when the number of associated clients reaches zero.
  - Disassociation messages are sent to new clients associating to 802.1X or web-authentication WLANs.
  - Controller-dependent activities such as 802.1X authentication, NAC, and web authentication (guest access) are disabled, and the AP does not send any Intrusion Detection System (IDS) reports to the controller.
  - Radio Resource Management (RRM) features (such as neighbor discovery; noise, interference, load, and coverage measurements, use of the neighbor list, and rogue containment and detection) are disabled. However, a FlexConnect AP supports dynamic frequency selection in standalone modes.

The FlexConnect AP maintains client connectivity even after entering standalone mode. However, once the AP reestablishes a connection with the controller, it disassociates all clients, applies new configuration information from the controller, and reallows client connectivity.

The LEDs on the AP change as the device enters different FlexConnect modes.

Related Topics

Supported Devices for FlexConnect, on page 70
Prerequisites for Using FlexConnect, on page 71
How FlexConnect Performs Authentication, on page 71
FlexConnect States, on page 72

FlexConnect States

The FlexConnect WLAN can be in any one of the following states depending on the configuration and state of controller connectivity:

- **Central authentication, central switching**—In this state, the controller handles client authentication, and all client data tunnels back to the controller. This state is valid only in connected mode.
- **Central authentication, local switching**—In this state, the controller handles client authentication, and the FlexConnect AP switches data packets locally. This state is supported only when the FlexConnect AP is in connected mode.
- **Local authentication, local switching**—In this state, the FlexConnect AP handles client authentication and switches client data packets locally. The authentication capabilities are present in the AP itself and

thus reduces the latency requirements. Local authentication can only be enabled on the WLAN of a FlexConnect AP that is in local switching mode.This state is valid in standalone mode and connected mode.

Local authentication is useful when the following conditions cannot be met:

- • A minimum bandwidth of 128 kbps.
  • Round trip latency no greater than 100 ms.
  • Maximum transmission unit (MTU) no smaller than 500 bytes.

Local authentication does not support:

- • Guest Authentication.
  • RRM information.
  • Local radius.
  • Roaming till the WLC and the other FlexConnect APs in the group are updated with the client information.

- **Authentication down, switching down**—In this state, the WLAN disassociates existing clients and stops sending beacon and probe responses. This state is valid only in standalone mode.
- **Authentication down, local switching**—In this state, the WLAN rejects any new clients trying to authenticate, but it continues sending beacon and probe responses to keep existing clients alive. This state is valid only in standalone mode.

The WLANS enter the following states when a FlexConnect AP enters the standalone mode:

- Local authentication, local switching state if the WLANs are configured as open, shared, WPA-PSK, or WPA2-PSK authentication and continue new client authentications.
- Authentication down, switching down state if the WLANs configured to central switching.
- Authentication down, local switching state if the WLANs configured to local-switch.

Related Topics

Supported Devices for FlexConnect, on page 70
Prerequisites for Using FlexConnect, on page 71
How FlexConnect Performs Authentication, on page 71
FlexConnect Operation Modes: Connected and Standalone, on page 72
How to Set Up and Use FlexConnect: Workflow, on page 73

How to Set Up and Use FlexConnect: Workflow

To configure FlexConnect, you must follow the instructions in this section in the following order:

1. Configure a Remote Switch for FlexConnect
2. Configure a Centrally-Switched WLAN Controller for FlexConnect
3. Configure a Locally-Switched WLAN Controller for FlexConnect
4. Configure a Centrally-Switched WLAN Controller for Guest Access
5. Configure FlexConnect on an AP
6. Connect Client Devices to the WLANs (FlexConnect)

Configure a Remote Switch for FlexConnect

To prepare the switch at the remote site, follow these steps:

Step 1 Connect the AP that is enabled for FlexConnect to a trunk or access port on the switch.

Step 2 Configure the switch to support the FlexConnect AP.

Related Topics

Example: Configure FlexConnect on Switches at Remote Sites, on page 74
Configure a Centrally-Switched WLAN Controller for FlexConnect, on page 75
Configure a Locally-Switched WLAN Controller for FlexConnect, on page 75
Configure a Centrally-Switched WLAN Controller for Guest Access, on page 76

Example: Configure FlexConnect on Switches at Remote Sites

In this sample configuration:

- The FlexConnect AP is connected to trunk interface FastEthernet 1/0/2 with native VLAN 100. The AP needs IP connectivity on the native VLAN.
- The remote site has local servers/resources on VLAN 101.
- A DHCP pool is created in the local switch for both VLANs in the switch.
- The first DHCP pool (NATIVE) is used by the FlexConnect AP, and the second DHCP pool (LOCAL-SWITCH) is used by the clients when they associate to a WLAN that is locally switched.

The addresses in this sample configuration are for illustration purposes only. The addresses that you use must fit into your upstream network.

```
ip dhcp pool NATIVE
   network 10.10.100.0 255.255.255.0
   default-router 10.10.100.1

!
ip dhcp pool LOCAL-SWITCH
   network 10.10.101.0 255.255.255.0
   default-router 10.10.101.1

!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 10.10.98.2 255.255.255.0
 spanning-tree portfast
!
interface FastEthernet1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 100,101
switchport mode trunk
 spanning-tree portfast
!
interface Vlan100
 ip address 10.10.100.1 255.255.255.0
 ip helper-address 10.10.100.1
!
interface Vlan101
 ip address 10.10.101.1 255.255.255.0
 ip helper-address 10.10.101.1
end
```

Related Topics

Configure a Remote Switch for FlexConnect, on page 73
Configure a Centrally-Switched WLAN Controller for FlexConnect, on page 75
Configure a Locally-Switched WLAN Controller for FlexConnect, on page 75
Configure a Centrally-Switched WLAN Controller for Guest Access, on page 76

Configure a Centrally-Switched WLAN Controller for FlexConnect

To create a centrally switched WLAN:

Step 1 Choose **Configuration > Network > Network Devices > Wireless Controllers**.

Step 2 Click the Device Name of the appropriate controller.

Step 3 From the left sidebar menu, choose **WLAN** > **WLAN Configuration** to access the WLAN Configuration page.

Step 4 Choose **Add a WLAN** from the Select a command drop-down list, and click Go.

Cisco APs can support up to 16 WLANs per controller. However, some Cisco APs do not support WLANs that have a WLAN ID greater than 8. In such cases when you attempt to create a WLAN the following message is displayed:

Not all types of AP support WLAN ID greater than 8, do you wish to continue?

Click OK to creates a WLAN with the next available WLAN ID.

If you have earlier deleted a WLAN that has a WLAN ID less than 8, then that ID is applied to the next created WLAN.

Step 5 Choose a template from the drop-down list to apply it to the controller.

To create a new WLAN template, click **Click here** link to be redirected to the template creation page.

Step 6 Choose **WPA1+WPA2** from the Layer 2 Security drop-down list.

Step 7 Check the **Status** check box under General Policies to enable the WLAN.

If NAC is enabled and you have created a quarantined VLAN for use with this, make sure to select it from the Interface drop-down list under General Policies. Also, check the **Allow AAA Override** check box to ensure that the controller validates a quarantine VLAN assignment.

Step 8 Click **Save.**

Related Topics

Configure a Remote Switch for FlexConnect, on page 73
Configure a Locally-Switched WLAN Controller for FlexConnect, on page 75
Configure a Centrally-Switched WLAN Controller for Guest Access, on page 76

Configure a Locally-Switched WLAN Controller for FlexConnect

To create a locally switched WLAN:

Step 1 Create a new WLAN as described in Configure a Centrally-Switched WLAN Controller for FlexConnect , Step 1 to Step 5.

Step 2 Click the WLAN ID and modify the configuration parameters.

Choose **WPA1+WPA2** from the Layer 2 Security drop-down list. Make sure you choose PSK authentication key management and enter a preshared key.

Step 3 Check the **Admin Status** check box to this WLAN.

Step 4 Check the FlexConnect **Local Switching** check box to enable local switching.

Step 5 Click **Save** to commit your changes.

Related Topics

Configure a Remote Switch for FlexConnect, on page 73
Configure a Centrally-Switched WLAN Controller for FlexConnect, on page 75
Configure a Centrally-Switched WLAN Controller for Guest Access, on page 76

Configure a Centrally-Switched WLAN Controller for Guest Access

To create a Centrally Switched WLAN for Guest Access to tunnel guest traffic to the controller:

Step 1 Create a new WLAN as described in *Configure a Centrally-Switched WLAN Controller for FlexConnect* , Step 1 to Step 5.

Step 2 Click the WLAN to modify the following configuration parameters:

a) Choose **None** from the Layer 2 Security and Layer 3 Security drop-down lists on the **Security** tab.
b) Check the **Web Policy** check box.
c) Select **Authentication**.
d) Configure a preauthentication access control list (ACL) on the WLAN if you are using an external web server, and then choose this ACL as the WLAN preauthentication ACL.

Step 3 Check the **Status** check box under General Policies to enable the WLAN.

Step 4 Click **Save** to commit your changes.

What to do next

Related Topics

- Configure a Remote Switch for FlexConnect
- Configure a Centrally-Switched WLAN Controller for FlexConnect
- Configure a Locally-Switched WLAN Controller for FlexConnect
- Configure a Centrally-Switched WLAN Controller for Guest Access
- (templates chapter)

Related Topics

Configure a Remote Switch for FlexConnect, on page 73
Configure a Centrally-Switched WLAN Controller for FlexConnect, on page 75
Configure a Locally-Switched WLAN Controller for FlexConnect, on page 75
Configure the Web Authentication Type for a Controller WLAN

Add Guests to a Centrally-Switched WLAN (FlexConnect)

To add a local user:

Step 1 **Configuration** > **Templates** > **Features & Technologies** , then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Select **Security** > **AAA** > **Local Net Users** from the left sidebar menu.

Step 3 Complete the required fields.

Step 4 From the **Profile** drop-down list, choose the appropriate SSID.

Step 5 Enter a description of the guest user account.

Step 6 Click **Save as New Template**.

Related Topics

Configure a Centrally-Switched WLAN Controller for Guest Access, on page 76

Configure FlexConnect on an AP

To configure an AP for FlexConnect, follow these steps:

Step 1 Add the AP physically to the network.

Step 2 Select **Configuration > Wireless technologies > Access Point Radios**.

Step 3 Select the AP from the AP Name list.

Step 4 Select **Configuration > Templates > Lightweight Acess Points** or **Autonomous Access Points** if the AP Mode field does not display FlexConnect.

If the AP Mode field displays FlexConnect skip to Step 8.

Step 5 Select the AP from the AP Name list. The Lightweight AP Template Detail page appears.

Step 6 Check the **FlexConnect Mode supported** check box to view all the profile mappings.

If you are changing the mode to FlexConnect and if the AP is not already in FlexConnect mode, all other FlexConnect parameters are not applied on the AP.

Step 7 Check **VLAN Support** check box and enter the number of the native VLAN on the remote network in the Native VLAN ID text box.

Step 8 Click the **Apply/Schedule** tab to save your changes.

Step 9 Click the **Edit** link in the Locally Switched VLANs section to change the number of VLANs from which a client IP address is obtained.

Step 10 Click **Save** to save your changes.

Repeat this procedure for any additional APs that need to be configured for FlexConnect at the remote site.

Related Topics

Configure a Remote Switch for FlexConnect, on page 73
Configure a Centrally-Switched WLAN Controller for FlexConnect, on page 75
Configure a Locally-Switched WLAN Controller for FlexConnect, on page 75

Connect Client Devices to the WLANs (FlexConnect)

Follow the instructions for your client device to create profiles that connect to the WLANs you created while configuring the controller.

In our example, you create three profiles on the client:

1. To connect to the centrally switched WLAN, create a client profile that uses WPA/WPA2 with PEAP-MSCHAPV2 authentication. When the client becomes authenticated, it gets an IP address from the management VLAN of the controller.
2. To connect to the locally switched WLAN, create a client profile that uses WPA/WPA2 authentication. When the client becomes authenticated, it gets an IP address from VLAN 101 on the local switch.
3. To connect to the centrally switched WLAN for Guest Access, create a profile that uses open authentication. When the client becomes authenticated, it gets an IP address from VLAN 101 on the network local to the AP. After the client connects, the local user types any HTTP address in the web browser. You are automatically directed to the controller to complete the web-authentication process. When the web login page appears, enter the username and password.

To see if data traffic of the client is being locally or centrally switched, choose **Monitor > Devices > Clients**.

Related Topics

Configure a Remote Switch for FlexConnect, on page 73
Configure a Centrally-Switched WLAN Controller for FlexConnect, on page 75
Configure a Locally-Switched WLAN Controller for FlexConnect, on page 75
Configure a Centrally-Switched WLAN Controller for Guest Access, on page 76

Create AP Groups to Use with FlexConnect

FlexConnect enables you to configure and control APs in a remote location through a wide area network (WAN) link without deploying a controller in each location. There is no deployment restriction on the number of FlexConnect APs per location, but you can organize and group the APs.

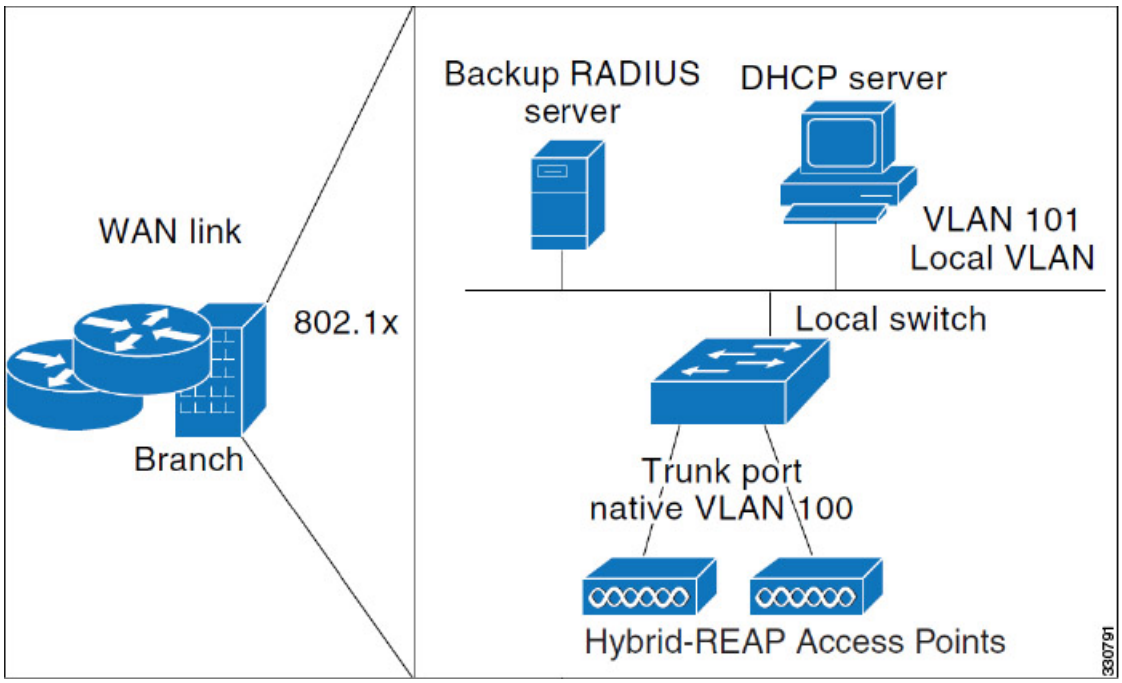
By forming AP groups with similar configurations, a procedure such as CCKM fast roaming can be processed faster than going through the controller individually.

For example, to activate CCKM fast roaming, the FlexConnect APs must know the CCKM cache for all devices that could associate with it. If you have a controller with 300 APs and 1000 devices that can potentially connect, it is quicker and more practical to process and send the CCKM cache for the FlexConnect group rather than for all 1000 devices. One particular FlexConnect group could focus on a small number of APs so that devices in that group connect to and roam between those few APs. With the established group, features such as CCKM cache and backup RADIUS are configured for the entire FlexConnect group rather than being configured in each AP.

All of the FlexConnect APs in a group share the same WLAN, backup RADIUS server, CCKM, and local authentication configuration information. This feature is helpful if you have multiple FlexConnect APs in a remote office or on the floor of a building and you want to configure them all at once. For example, you can configure a backup RADIUS server for a FlexConnect group rather than having to configure the same server on each AP.

The following figure illustrates a typical FlexConnect group deployment with a backup RADIUS server in the branch office.

Figure 9: FlexConnect Group Deployment



Related Topics

- FlexConnect Groups and Backup RADIUS Servers
- FlexConnect Groups and CCKM
- FlexConnect Groups and Local Authentication
- Audit Controller FlexConnect AP Groups to Locate Configuration Differences

FlexConnect Groups and Backup RADIUS Servers

You can configure the controller to allow a FlexConnect AP in standalone mode to perform full 802.1x authentication to a backup RADIUS server. You can either configure a primary RADIUS server or both a primary and secondary RADIUS server.

Related Topics

- FlexConnect Groups and CCKM
- FlexConnect Groups and Local Authentication
- Audit Controller FlexConnect AP Groups to Locate Configuration Differences

FlexConnect Groups and CCKM

FlexConnect groups are required for CCKM fast roaming. When you configure your WLAN for CCKM fast secure roaming, EAP-enabled clients securely roam from one access point to another without the need to re-authenticate with the RADIUS server. Using CCKM, an access point uses a fast re-keying technique that enables Cisco client devices to roam from one access point to another typically in under 150 milliseconds. CCKM fast secure roaming ensures that there is no perceptible delay in time-sensitive applications. The

FlexConnect access points obtains the CCKM cache information for all the clients that might associate so they can process it quickly instead of sending it back to the controller.

For example, if you have a controller with 300 APs and 100 clients that might associate, sending the CCKM cache for all 100 clients is not practical. If you create a FlexConnect group comprising a limited number of APs, the clients roam only among those four APs, and the CCKM cache is distributed among those four APs only when the clients associate to one of them.

CCKM fast roaming between FlexConnect and non-FlexConnect APs is not supported.

Related Topics

- FlexConnect Groups and Backup RADIUS Servers
- FlexConnect Groups and Local Authentication
- Audit Controller FlexConnect AP Groups to Locate Configuration Differences

FlexConnect Groups and Local Authentication

You can configure the controller to allow a FlexConnect AP in standalone mode to perform LEAP or EAP-FAST authentication for up to 20 statically configured users. The controller sends the static list of usernames and passwords to each FlexConnect AP when it joins the controller. Each AP in the group authenticates only its own associated clients.

This feature is ideal for customers who are migrating from an autonomous AP network to a lightweight FlexConnect AP network and are not interested in maintaining a large user database nor adding another hardware device to replace the RADIUS server functionality available in the autonomous AP.

LEAP or EAP-FAST authentication can be used in conjunction with the FlexConnect backup RADIUS server. If a FlexConnect group is configured with both a backup RADIUS server and local authentication, the FlexConnect AP always attempts to authenticate clients using the primary backup RADIUS server first, followed by the secondary backup RADIUS server (if the primary is not reachable), and finally the FlexConnect AP itself (if the primary and secondary RADIUS servers are not reachable).

Related Topics

- FlexConnect Groups and Backup RADIUS Servers
- FlexConnect Groups and CCKM
- Audit Controller FlexConnect AP Groups to Locate Configuration Differences

View Existing FlexConnect AP Groups

You can view a list of existing FlexConnect AP groups. To verify that an individual AP belongs to a FlexConnect group, click the **Users configured in the group** link. It takes you to the FlexConnect AP Group page, which shows the names of the groups and the APs that belong to it.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **FlexConnect** > **FlexConnect AP Groups**. The FlexConnect AP Groups page opens.

Step 4 Click the group name to view details about the FlexConnect AP group.

Related Topics

Audit Controller WLAN AP Groups to Locate Configuration Differences , on page 68

Configure FlexConnect AP Groups

To configure a FlexConnect AP group, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **FlexConnect** > **FlexConnect AP Groups**.

Step 4 From the Select a command drop-down list, click **Add FlexConnect AP Group** to open the **FlexConnect AP Group > Add From Template** pane.

Step 5 Choose a template from the **Select a template to apply to this controller** drop-down list.

Step 6 Click **Apply**.

Step 7 Configure the required FlexConnect AP Group parameters. You can add, edit, or remove any of the following mappings by clicking the required tab:

- VLAN-ACL Mapping—Valid VLAN ID range is 1-4094.
- WLAN-ACL Mapping—Select the FlexConnect access control list for external web authentication. You can add up to a maximum of 16 WebAuth ACLs.
- WebPolicy ACL—Select the FlexConnect access control list to be added as a web policy. You can add up to a maximum of 16 Web-Policy ACLs.
- Local Split
- Central DHCP
  - Central DHCP—When you enable this feature, the DHCP packets received from APs are centrally switched to the controller and then forwarded to the corresponding VLAN based on the AP and the SSID.
  - Override DNS—You can enable or disable the overriding of the DNS server address on the interface assigned to the locally switched WLAN. When you override DNS in centrally switched WLANs, the clients get their DNS server IP address from the AP, not from the controller.
  - NAT-PAT—You can enable or disable Network Address Translation (NAT) and Port Address Translation (PAT) on locally switched WLANs. You must enable Central DHCP Processing to enable NAT and PAT.

Step 8 To see if an individual access point belongs to a FlexConnect group, click the **Users configured in the group** link. The FlexConnect AP Group page shows the names of the groups and the access points that belong in it.

Step 9 Click **Save**.

Step 10 To delete an existing FlexConnect AP group, select the check box of the group you want to remove, and choose **Delete FlexConnect AP Group** from the **Select a command** drop-down list.

Related Topics

View Existing FlexConnect AP Groups, on page 80

Audit Controller FlexConnect AP Groups to Locate Configuration Differences

If the FlexConnect configuration changes over a period of time either on Cisco Prime Infrastructure or the controller, you can audit the configuration. The changes are visible on subsequent screens. You can choose to synchronize the configuration by refreshing Cisco Prime Infrastructure or the controller.

Related Topics

Configure FlexConnect AP Groups, on page 81
View Existing FlexConnect AP Groups, on page 80

Default FlexConnect Group

Default FlexConnect Group is a container where FlexConnect APs, which are not part of any administrator configured FlexConnect group, are added automatically when they join the controller. The Default FlexConnect Group is created and stored when the controller comes up (after upgrading from a previous release). You cannot add or delete this group manually. Also, you cannot manually add or delete access points to the Default FlexConnect Group. The APs in Default FlexConnect Group inherits the common configuration of the group. Any change in the group configuration is propagated to all the APs in the group.

When an administrator created group is deleted, all the APs from that group are moved to the Default FlexConnect Group and inherits the configuration of this group. Similarly, APs removed manually from other groups are also added to the Default FlexConnect Group.

When an AP from the Default FlexConnect Group is added to a customized group, the existing configuration (from Default FlexConnect Group) is deleted and the configuration from the customized group is pushed to the AP. If there is a standby controller, the Default FlexConnect Group and its configuration is also synchronized to it.

When an AP is converted from local to FlexConnect mode, and if it is not part of any administrator configured FlexConnect group, then it becomes part of Default FlexConnect group.

Note Efficient AP Image Upgrade feature is not supported with the Default FlexConnect AP group.

Related Topics

- Move APs from Default FlexConnect AP Group to another FlexConnect Group
- Default FlexConnect Group

Move APs from Default FlexConnect AP Group to another FlexConnect Group

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **FlexConnect** > **FlexConnect AP Groups**.

Step 4 From the FlexConnect AP Groups, click the Group Name.

Step 5 In the **FlexConnect AP** tab, click + Add AP. The Add FlexConnect AP page shows the APs from the default FlexConnect group.

Step 6 Select any of the AP Name and click **Add**.

The selected AP will automatically added to the new group and gets deleted from the default FlexConnect group.

Step 7 Click **Save**.

Related Topics

Default FlexConnect Group, on page 82

Delete FlexConnect AP Group

Note You cannot delete the default FlexConnect group.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **FlexConnect** > **FlexConnect AP Groups**.

Step 4 Click a Group Name and select **Delete FlexConnect AP Group** from the **Select a Command** drop-down list.

Step 5 Click **OK** to confirm the deletion.

Related Topics

Default FlexConnect Group, on page 82
Configure and Monitor APs Using FlexConnect, on page 70

Configure Security Settings for a Controller or Device

- Configure Client Exclusion Policies on Controllers
- View Cisco-Supplied IDS Signatures Applied to Controllers
- Create Custom IDS Signatures
- Configure a Controller's AP Authentication and Management Frame Protection
- Configure a Access Control List

Configure TFTP File Encryption for a Controller

You can configure file encryption to ensure that data is encrypted when you upload or download controller configuration files from a TFTP server.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **File Encryption**.

Step 4 Check the **File Encryption** check box.

Step 5 In the **Encryption Key** field, enter a text string of exactly 16 characters. Reenter the key in the **Confirm Encryption Key** field.

Step 6 Click **Save**.

Related Topics

Configure Security Settings for a Controller or Device, on page 83

Configure AAA Security for a Controller

This section describes how to configure controller security AAA parameters and contains the following topics:

- Configure Controller AAA General Parameters
- View Controller AAA RADIUS Auth Servers
- View Controller AAA RADIUS Acct Servers
- Configure AAA RADIUS Fallback Parameters on a Controller
- Configure AAA LDAP Servers on a Controller
- Configure AAA TACACS Servers on a Controller, on page 89
- View Controller AAA Local Net Users
- Configure AAA MAC Filtering on a Controller
- Configure AAA AP/MSE Authorization on a Controller
- Configure AAA Web Auth on a Controller

Configure Controller AAA General Parameters

The General page allows you to configure the local database entries on a controller.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **AAA** > **General - AAA**.

Step 4 Enter the maximum number of allowed database entries. The valid range is 512 - 2048.

Step 5 In the Mgmt User Re-auth Interval, set the termination interval for management users.

Step 6 Reboot your server to apply the changes.

Related Topics

Configure AAA Security for a Controller, on page 84

View Controller AAA RADIUS Auth Servers

You can view a summary of existing RADIUS authentication servers

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **AAA** > **RADIUS Auth Servers**. The following RADIUS Auth Servers parameters appear:

- Server Index—Access priority number for the RADIUS server (display only). Click to go to Configure IPaddr > RADIUS Authentication Server.
- Server Address—IP address of the RADIUS server (read-only).
- Port Number—Controller port number (read-only).
- Admin Status—Enable or Disable.
- Network User—Enable or Disable.
- Management User—Enable or Disable.

Related Topics

Configure AAA Security for a Controller, on page 84
Add AAA Auth Servers to a Controller, on page 85

Add AAA Auth Servers to a Controller

To add an authentication server, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **AAA** > **RADIUS Auth Servers**.

Step 4 From the Select a command drop-down list, choose **Add Auth Server** to open the Radius Authentication Server > Add From Template page.

Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 Click **Apply**.

To create a new template for Radius authentication servers, choose **Configuration** > **Templates** > **Features and Technologies**.

Related Topics

Configure AAA Security for a Controller, on page 84
View Controller AAA RADIUS Acct Servers, on page 86

View Controller AAA RADIUS Acct Servers

To view a summary of existing RADIUS accounting servers, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **AAA** > **RADIUS Acct Servers**. RADIUS Acct Server parameters include the following:

- Server Index—Access priority number for the RADIUS server (read-only). Click to open the Radius Acct Servers Details page.
- To edit or audit the current accounting server parameters, click the Server Index for the applicable accounting server.
- Server Address—IP address of the RADIUS server (read-only).
- Port Number—Controller port number (read-only).
- Admin Status—Enable or Disable.
- Network User—Enable or Disable.

Related Topics

Configure AAA Security for a Controller, on page 84
Add an AAA Accounting Server to a Controller, on page 86

Add an AAA Accounting Server to a Controller

To add an accounting server, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > RADIUS Acct Servers**.

Step 4 From the **Select a command** drop-down list, choose **Add Acct Server** to open the Radius Acct Servers Details > Add From Template page.

Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 From the drop-down list, choose a controller on which to apply to this template.

Step 7 Click **Apply**.

To create a new template for Radius accounting servers, choose **Configuration > Templates > Features and Technologies > Controller > Security > AAA > RADIUS Acct Servers**.

Related Topics

Configure AAA Security for a Controller, on page 84
View Controller AAA RADIUS Acct Servers, on page 86

Delete an AAA Accounting Server from a Controller

To delete an accounting server, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **AAA** > **RADIUS Acct Servers**.

Step 4 Select the check box(es) for the applicable accounting server(s).

Step 5 From the **Select a command** drop-down list, choose **Delete Acct Server**.

Step 6 Click **Go**.

Step 7 Click **OK** in the pop-up dialog box to confirm the deletion.

Related Topics

Configure AAA Security for a Controller, on page 84
View Controller AAA RADIUS Acct Servers, on page 86

Configure AAA RADIUS Fallback Parameters on a Controller

To configure RADIUS fallback parameters, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **AAA** > **RADIUS Fallback**.

Step 4 Make the required changes, then click **Save**.

Step 5 Click **Audit** to check the present configuration status of Cisco Prime Infrastructure and the controller.

Related Topics

Configure AAA Security for a Controller, on page 84

Configure AAA LDAP Servers on a Controller

You can add and delete LDAP servers to controllers. Prime Infrastructure supports LDAP configuration for both an anonymous or authenticated bind.

To access the LDAP Servers page, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **AAA** > **LDAP Servers**.

This page displays LDAP servers currently used by this controller and contains the following parameters:

- Check box—Select the check box to choose an LDAP server for deletion.
- Server Index—A number assigned to identify the LDAP server. Click the index number to go the LDAP server configuration page.
- Server Address—The LDAP server IP address.
- Port Number—The port number used to communicate with the LDAP server.
- Admin Status—Server template status.
- Indicates if use of the LDAP server template is enabled or disabled.

Step 4 Click on a column title to toggle whether the information in sorted in ascending or descending order.

Related Topics

Configure AAA Security for a Controller, on page 84
Configure New AAA LDAP Bind Requests on a Controller, on page 89

Add AAA LDAP Servers to a Controller

To add an LDAP Server, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **AAA** > **LDAP Servers**.

Step 4 From the Select a command drop-down list, choose **Add LDAP Server**.

Step 5 Click **Go**.

Related Topics

Configure AAA Security for a Controller, on page 84

Delete AAA LDAP Servers from a Controller

To delete the LDAP Server, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **AAA** > **LDAP Servers**.

Step 4 Select the check box(es) of the LDAP servers that you want to delete.

Step 5 From the **Select a command** drop-down list, choose **Delete LDAP Servers**.

Step 6 Click **Go**.

Related Topics

Configure AAA Security for a Controller, on page 84

Configure New AAA LDAP Bind Requests on a Controller

Prime Infrastructure supports LDAP configuration for both an anonymous or authenticated bind. A bind is a socket opening that performs a lookup.

To configure LDAP bind requests, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **AAA** > **LDAP Servers**.

Step 4 Click a value under the Server Index column.

Step 5 From the Bind Type drop-down list, choose **Authenticated** or **Anonymous**. If you choose Authenticated, you must enter a bind username and password as well.

Step 6 In the Server User Base DN text box, enter the distinguished name of the subtree in the LDAP server that contains a list of all the users.

Step 7 In the Server User Attribute text box, enter the attribute that contains the username in the LDAP server.

Step 8 In the Server User Type text box, enter the ObjectType attribute that identifies the user.

Step 9 In the Retransmit Timeout text box, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

Step 10 Select the **Admin Status** check box if you want the LDAP server to have administrative privileges.

Step 11 Click **Save**.

Related Topics

Configure AAA Security for a Controller, on page 84

Configure AAA TACACS Servers on a Controller

You can delete TACACS+ servers from the controllers. To access the TACACS+ Servers page, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **TACACS+ Servers**.

This page displays TACACS+ servers currently used by this controller and contains the following parameters:

- Check box—Select the check box to choose a TACACS+ server for deletion.
- Server Type—The TACACS+ server type—accounting, authorization, or authentication.

- Server Index—A number assigned to identify the TACACS+ server and set its use priority. Click the index number to go the TACACS+ server configuration page.
- Server Address—The TACACS+ server IP address.
- Port Number—The port number used to communicate with the TACACS+ server.
- Admin Status—Server template status. Indicates if use of the TACACS+ server template is enabled.

Step 4 Choose **Delete TACACS+ Servers** from the **Select a command** drop-down list, then click **Go** to delete all TACACS+ servers with a selected check box from the controller.

Step 5 Click on a column title to toggle whether the information in sorted in ascending or descending order.

Related Topics

Configure AAA Security for a Controller, on page 84

View Controller AAA Local Net Users

You can view summary of the existing local network user controllers for clients who are allowed to access a specific WLAN. This is an administrative bypass of the RADIUS authentication process. Layer 3 Web Authentication must be enabled. The client information is passed to the RADIUS authentication server first, and if the client information does not match a RADIUS database entry, this local database is polled. Clients located in this database are granted access to network services if the RADIUS authentication fails or does not exist.

To view existing local network users, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **AAA** > **Local Net Users**. The Local Net Users page displays the following local net user parameters:

- Username—User-defined identification.
- WLAN ID—Any WLAN ID, 1 through 16; 0 for all WLANs; 17 for third-party WLAN that this local net user is allowed to access.
- Description—Optional user-defined description.

Related Topics

Configure Local EAP on a Controller, on page 94
Delete AAA Local Net Users from a Controller, on page 90

Delete AAA Local Net Users from a Controller

To delete a local net user, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **AAA** > **Local Net Users**.

Step 4 Select the check box(es) for the applicable local net user(s).

Step 5 From the Select a command drop-down list, choose **Delete Local Net Users**.

Step 6 Click **Go**.

Step 7 Click **OK** in the dialog box to confirm the deletion.

Related Topics

Configure AAA Security for a Controller, on page 84

Configure AAA MAC Filtering on a Controller

You can view MAC Filter information. You cannot use MAC address in the broadcast range.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **AAA** > **MAC Filtering**. The MAC Filtering page displays the following parameters:

- MAC Filter Parameters
  - RADIUS Compatibility Mode—User-defined RADIUS server compatibility: Cisco ACS, FreeRADIUS, or Other.
  - MAC Delimiter—The MAC delimiters can be Colon (xx:xx:xx:xx:xx:xx), Hyphen (xx-xx-xx-xx-xx-xx), Single Hyphen (xxxxxx-xxxxxx), or No Delimiter (xxxxxxxxxxxx), as required by the RADIUS server.
- MAC Filters
  - MAC Address—Client MAC address. Click to open Configure *IPaddr* > MAC Filter.
  - WLAN ID—1 through 16, 17 = Third-party AP WLAN, or 0 = all WLANs.
  - Interface—Displays the associated Interface Name.
  - Description—Displays an optional user-defined description.

Step 4 From the Select a command drop-down list, choose **Add MAC Filters** to add a MAC Filter, **Delete MAC Filters** to delete the template(s), or **Edit MAC Filter** Parameters to edit the MAC Filters.

Step 5 Click **Go**.

Related Topics

Configure AAA Security for a Controller, on page 84

Configure AAA AP/MSE Authorization on a Controller

The AP/MSE Authorization page displays the access point policies and the list of authorized access points along with the type of certificate that an access point uses for authorization.

You cannot use MAC address in the broadcast range.

To access the AP/MSE Authorization page, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **AAA** > **AP or MSE Authorization**. The AP/MSE Authorization page displays the following parameters:

- AP Policies
  - Authorize APs—Enabled or Disabled.
  - Accept SSC-APs—Enabled or Disabled.
- AP/MSE Authorization
  - AP/MSE Base Radio MAC Address—The MAC address of the authorized access point. Click the AP/MSE Base Radio MAC Address to view AP/MSE Authorization details.
  - Type
  - Certificate Type—MIC or SSC.
  - Key Hash—The 40-hex long SHA1 key hash. The key hash is displayed only if the certificate type is SSC.

Related Topics

Configure AAA Security for a Controller, on page 84
Edit AAA AP/MSE Policies on a Controller, on page 92

Edit AAA AP/MSE Policies on a Controller

To edit AP/MSE Authorization access point policies, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **AAA** > **AP or MSE Authorization**.

Step 4 From the **Select a command** drop-down list, select **Edit AP Policies**, then click **Go**.

Step 5 Edit the following parameters, if necessary:

- **Authorize APs**—Select the check box to enable access point authorization.
- **Accept SSC-APs**—Select the check box to enable the acceptance of SSE access points.

Step 6 Click **Save** to confirm the changes, **Audit** to perform an audit on these device values, or **Cancel** to close this page with no changes.

Related Topics

Configure AAA Security for a Controller, on page 84

Configure AAA Web Auth on a Controller

The Web Auth Configuration page enables the user to configure the web auth configuration type. If the type is configured as customized, the user downloaded web auth replaces the controller-provided internal web auth page.

To access the Web Auth Configuration page, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **AAA** > **Web Auth Configuration**.

Step 4 Select the Web Auth Type from the drop-down list.

Step 5 Configure the web auth parameters depending on the type chosen:

- Default Internal
  - Custom Redirect URL—URL where the user is redirected after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user is directed to the company home page.
  - Logo Display—Enable or disable logo display.
  - Web Auth Page Title—Title displayed on web authentication page.
  - Web Auth Page Message—Message displayed on web authentication page.
- Customized Web Auth

  You can download an example login page and customizing the page. If you are using a customized web authentication page, it is necessary to download the example login.tar bundle file from the server, edit the login.html file and save it as either a .tar or .zip file, then download the .tar or .zip file to the controller.

  Click the preview image to download this sample login page as a TAR. After editing the HTML you might click here to redirect to the Download Web Auth page. See the Download Compressed Web Authorization Login Page Information to Controllers for more information.
- External
  - External Redirect URL—Location of the login.html on an external server on the network.

    If there are not any external web auth servers configured, you have the option of configuring one.

Configure an AAA Password Policy on a Controller

This page enables you to determine your password policy.

To make modifications to an existing password policy, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type> Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **AAA** > **Password Policy**.

Step 4 Modify the password policy parameters as appropriate.

Step 5 Click **Save**.

If you disable password policy options, you see a "Disabling the strong password check(s) will be a security risk as it allows weak passwords" message.

Related Topics

Configure AAA Security for a Controller, on page 84

Configure Local EAP on a Controller

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down.

When you enable local EAP, the controller serves as the authentication server and the local user database, making it independent of an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users.

Related Topics

Configure Local EAP General Parameters on a Controller, on page 94
View the Local EAP Profiles Used By a Controller, on page 95
Configure Local EAP General EAP-Fast Parameters on a Controller
Configure Local EAP General Network Users Priority on a Controller, on page 96

Configure Local EAP General Parameters on a Controller

You can specify a timeout value for local EAP. You can then add a template with this timeout value or make changes to an existing template.

If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then re-authenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP.

To specify a timeout value for local EAP, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **Local EAP** > **General - Local EAP**.

Step 4 Enter the Local Auth Active Timeout in the Local Auth Active Timeout text box (in seconds). Local Auth Active Timeout refers to the timeout period during which Local EAP is always used after all Radius servers are failed.

Step 5 The following values should be adjusted if you are using EAP-FAST, manual password entry, one-time password, or 7920/7921 phones.

You must increase the 802.1x timeout values on the controller (default=2 seconds) for the client to obtain the PAC using automatic provisioning. We recommend the default timeout on the Cisco ACS server of 20 seconds.

- Local EAP Identify Request Timeout =1 (in seconds)
- Local EAP Identity Request Maximum Retries=20 (in seconds)
- Local EAP Dynamic Wep Key Index=0
- Local EAP Request Timeout=20 (in seconds)
- Local EAP Request Maximum Retries=2
- EAPOL-Key Timeout=1000 (in milli-seconds)
- EAPOL-Key Max Retries=2
- Max-Login Ignore Identity Response

Roaming fails if these values are not set the same across multiple controllers.

Step 6 Click **Save**.

Related Topics

Configure Local EAP on a Controller, on page 94
View the Local EAP Profiles Used By a Controller, on page 95
Configure Local EAP General EAP-Fast Parameters on a Controller
Configure Local EAP General Network Users Priority on a Controller, on page 96

View the Local EAP Profiles Used By a Controller

You can apply a template for a local EAP profile or make modifications to an existing template.

The LDAP backend database supports only these local EAP methods: EAP-TLS and EAP-FAST with certificates. LEAP and EAP-FAST with PACs are not supported for use with the LDAP backend database.

To view existing local EAP profiles, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **Local EAP** > **Local EAP Profiles**. The Local EAP Profiles page displays the following parameters:

- EAP Profile Name—User-defined identification.
- LEAP—Authentication type that leverages Cisco Key Integrity Protocol (CKIP) and MMH message integrity check (MIC) for data protection. A username and password are used to perform mutual authentication with the RADIUS server through the access point.
- EAP-FAST—Authentication type (Flexible Authentication via Secure Tunneling) that uses a three-phased tunnel authentication process to provide advanced 802.1x EAP mutual authentication. A username, password, and PAC (protected access credential) are used to perform mutual authentication with the RADIUS server through the access point.
- TLS—Authentication type that uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It requires a client certificate for authentication.
- PEAP—Protected Extensible Authentication Protocol.

Related Topics

Configure Local EAP on a Controller, on page 94
Add Local EAP Profiles to a Controller, on page 96

Add Local EAP Profiles to a Controller

To add a local EAP profile, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **Local EAP** > **Local EAP Profile**.

Step 4 From the **Select a command** drop-down list, choose **Add Local EAP Profile**.

Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 Click **Apply**.

Related Topics

Configure Local EAP on a Controller, on page 94
Configure Local EAP General Parameters on a Controller, on page 94
View the Local EAP Profiles Used By a Controller, on page 95
Configure Local EAP General EAP-Fast Parameters on a Controller
Configure Local EAP General Network Users Priority on a Controller, on page 96

Configure Local EAP General Network Users Priority on a Controller

To specify the order that LDAP and local databases use to retrieve user credential information, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Devices Groups menu on the left, select **Device Type> Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **Local EAP** > **Network Users Priority**

Step 4 Use the left and right pointing arrows to include or exclude network credentials in the right-most list.

Step 5 Use the up and down buttons to determine the order credentials are attempted.

Step 6 Click **Save**.

Related Topics

Configure Local EAP on a Controller, on page 94
Configure Local EAP General Parameters on a Controller, on page 94
Configure a Controller's Web Auth Certificates, on page 97
Configure IP Sec CA Certificates on Controllers, on page 101

Configure a Controller's Web Auth Certificates

You can download a web authorization certificate or regenerate the internally-generated web auth certificate.

Caution Each certificate has a variable-length embedded RSA Key. The RSA key can vary from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a certificate authority (such as the Microsoft CA), make sure the RSA key embedded in the certificate is at least 768 Bits.

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > Web Auth Certificate**.

Step 4 Click **Download Web Auth Certificate** to access the Download Web Auth Certificate to Controller page.

Related Topics

Configure Local EAP General Parameters on a Controller, on page 94
Configure Local EAP on a Controller, on page 94

Configure a Controller User Login Policies

To configure the user login policies for controllers, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > User Login Policies.**

Step 4 Enter the maximum number of concurrent logins allowed for a single username.

Step 5 Click **Save**.

Configure a Device's Manually Disabled Clients

The Disabled Clients page enables you to view excluded (blocklisted) client information.

Clients who fail to authenticate three times when attempting to associate are automatically blocked, or excluded, from further association attempts for an operator-defined timeout. After the Excluded timeout, the client is allowed to retry authentication until it associates or fails authentication and is excluded again.

You cannot use MAC address in the broadcast range.

To access the Manually Disabled Clients page, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > Manually Disabled Clients**. The Manually Disabled Clients page displays the following parameters:

- MAC Address—Disabled Client MAC addresses. Click a list item to edit the disabled client description.
- Description—Optional description of disabled client.

Configure a Controller's Access Control Lists (ACLs)

You can view, edit, or add a new access control list (ACLs) for controllers.

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > Access Control Lists.**

a) Check the check box to delete one or more ACLs

or

b) Click an ACL item to view its parameters.

Configure Controller ACL Rules, on page 98
Add ACL Security for Controller CPUs, on page 100

Configure Controller ACL Rules

You can create and modify access control list Access Control Lists (ACL) rules applied to controllers.

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > Access Control Lists**.

Step 4 Click an ACL name to view and modify the parameters.

Step 5 Optionally check the check box to access control list rules.

Create New Controller ACL Rules

Step 1 Choose **Device Type** > **Wireless Controller**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **Access Control Lists**.

Step 4 Click an ACL name.

Step 5 Click an applicable Seq#, or choose **Add New Rule** to access this page.

Configure Controller ACL Rules, on page 98
Add ACL Security for Controller CPUs, on page 100

Configure FlexConnect ACL Security for Controllers

The ACLs on FlexConnect provide a mechanism to cater to the need for access control at the FlexConnect access point for protection and integrity of locally switched data traffic from the access point.

Add FlexConnect ACLs on Controllers, on page 99
Delete FlexConnect ACLs for Controllers, on page 99

Add FlexConnect ACLs on Controllers

To add an Access Control List for FlexConnect access points, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > FlexConnect ACLs**.

Step 4 From the Select a command drop-down list, choose **Add FlexConnect ACLs**.

Step 5 Click **Go**.

You cannot add a FlexConnect ACL if there is no template created. If you try to create an FlexConnect ACL when there are no templates available, you are redirected to the New Controller Templates page where you can create a template for FlexConnect ACL.

Step 6 Choose a template from the drop-down list to apply to the controller, and click **Apply**.

The FlexConnect ACL that you created appears in Configure > Controllers > *IP Address* > Security > FlexConnect ACLs.

Configure FlexConnect ACL Security for Controllers, on page 99

Delete FlexConnect ACLs for Controllers

To delete a FlexConnect ACL, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller** .

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **FlexConnect ACLs**.

Step 4 From the FlexConnect ACLs page, select one or more FlexConnect ACLs to delete.

Step 5 From the Select a command drop-down list, choose **Delete FlexConnect ACLs**.

Step 6 Click **Go**.

Configure FlexConnect ACL Security for Controllers, on page 99

Add ACL Security for Controller CPUs

Access control lists (ACLs) can be applied to the controller CPU to control traffic to the CPU.

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > CPU Access Control Lists**.

Step 4 Select the **Enable CPU ACL** check box to enable the CPU ACL. The following parameters are available:

- ACL Name—Choose the ACL to use from the ACL Name drop-down list.
- CPU ACL Mode—Choose which data traffic direction this CPU ACL list controls.

Configure FlexConnect ACL Security for Controllers, on page 99
Configure a Controller’s Access Control Lists (ACLs), on page 98
Configure Controller ACL Rules, on page 98

View a Controller's Configured IDS Security Sensors

When the sensors identify an attack, they alert the controller to shun the offending client. When you add a new IDS (Intrusion Detection System) sensor, you register the controller with that IDS sensor so that the sensor can send shunned client reports to the controller. The controller also polls the sensor periodically.

To view IDS sensors, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **IDS Sensor Lists**.

The IDS Sensor page lists all IDS sensors that have been configured for this controller. Click an IP address to view details for a specific IDS sensor.

Configure IP Sec CA Certificates on Controllers

A Certificate Authority (CA) certificate is a digital certificate issued by one certificate authority (CA) for another certification CA.

Import IP Sec Certificates to Controllers, on page 101
Paste IP Sec Certificates to Controllers, on page 101

Import IP Sec Certificates to Controllers

To import a CA certificate from a file, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **IP Sec Certificates** > **CA Certificate**.

Step 4 Click **Browse** to navigate to the applicable certificate file.

Step 5 Click **Open**, then click **Save**.

Configure IP Sec CA Certificates on Controllers, on page 101

Paste IP Sec Certificates to Controllers

To paste a CA certificate directly, follow these steps:

Step 1 Copy the CA certificate to your computer clipboard.

Step 2 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 3 Click the device name of the applicable controller.

Step 4 From the left sidebar menu, choose **Security** > **IP Sec Certificates** > **CA Certificate**.

Step 5 Select the **Paste** check box.

Step 6 Paste the certificate directly into the text box.

Step 7 Click **Save**.

Configure IP Sec CA Certificates on Controllers, on page 101
Configure Network Identity (ID) Certificates on Controllers, on page 101
Configure a Controller's Web Auth Certificates, on page 97

Configure Network Identity (ID) Certificates on Controllers

This page lists the existing network Identity (ID) certificates by certificate name. An ID certificate can be used by web server operators to ensure secure server operation. ID certificates are available only if the controller is running Cisco Unified Wireless Network Software Version 3.2 or higher.

Import IP Sec Certificates to Controllers, on page 101
Paste IP Sec Certificates to Controllers, on page 101

Import ID Certificates to Controllers

To import an ID certificate from a file, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Configuration** > **Network** > **Network Devices**.
Step 2 Click the device name of the applicable controller.
Step 3 From the left sidebar menu, choose **Security** > **IP Sec Certificates** > **ID Certificate**.
Step 4 From the Select a command drop-down list, choose **Add Certificate**.
Step 5 Click **Go**.
Step 6 Enter the Name and Password.
Step 7 Click **Browse** to navigate to the applicable certificate file.
Step 8 Click **Open**, then click **Save**.

Configure Network Identity (ID) Certificates on Controllers, on page 101

Paste ID Certificates to Controllers

To paste an ID certificate directly, follow these steps:

Step 1 Copy the ID certificate to your computer clipboard.
Step 2 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.
Step 3 Click the device name of the applicable controller.
Step 4 From the left sidebar menu, choose **Security** > **IP Sec Certificates** > **ID Certificate**.
Step 5 From the Select a command drop-down list, choose **Add Certificate**.
Step 6 Click **Go**.
Step 7 Enter the Name and Password.
Step 8 Select the **Paste** check box.
Step 9 Paste the certificate directly into the text box.
Step 10 Click **Save**.

Configure IP Sec CA Certificates on Controllers, on page 101
Configure Network Identity (ID) Certificates on Controllers, on page 101

Configure Wireless Protection Policies on Controllers

This section describes the wireless protection policy configurations and contains the following topics:

• Configure a Controller's AP Authentication and Management Frame Protection

Configure Rogue AP Policies on Controllers

You can set up policies for rogue access points. Make sure that rogue detection is enabled on the desired access points. Rogue detection is enabled by default for all access points joined to a controller (except for OfficeExtend access points). However, in Cisco Prime Infrastructure software Release 6.0 or later, you can enable or disable rogue detection for individual access points by selecting or unselecting the **Rogue Detection** check box in the Access Point Details page.

Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices

To access the Rogue Policies page, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **Wireless Protection Policies** > **Rogue Policies**. The following parameters appear:

- Rogue Location Discovery Protocol—RLDP determines whether or not the rogue is connected to the enterprise wired network. Choose one of the following from the drop-down list:
  - Disable—Disables RLDP on all access points. This is the default value.
  - All APs—Enables RLDP on all access points.
  - Monitor Mode APs—Enables RLDP only on access points in monitor mode.
- Rogue APs
  - Expiration Timeout for Rogue AP and Rogue Client Entries (seconds)—Enter the number of seconds after which the rogue access point and client entries expire and are removed from the list. The valid range is 240 to 3600 seconds and the default value is 1200 seconds.

    If a rogue access point or client entry times out, it is removed from the controller only if its rogue state is Alert or Threat for any classification type.
  - Rogue Detection Report Interval—Enter the time interval in seconds at which the APs should send the rogue detection report to the controller. Valid range is 10 seconds to 300 seconds, and the default value is 10 seconds. This feature is applicable to APs that are in monitor mode only.
  - Rogue Detection Minimum RSSI—Enter the minimum RSSI value that a rogue should have for the APs to detect and for the rogue entry to be created in the controller. Valid range is -70 dBm to -128 dBm, and the default value is -128 dBm. This feature is applicable to all the AP modes.

    There can be many rogues with very weak RSSI values that do not provide any valuable information in the rogue analysis. Therefore, you can use this option to filter the rogues by specifying the minimum RSSI value at which the APs should detect rogues.
  - Rogue Detection Transient Interval—Enter the time interval at which a rogue has to be consistently scanned for by the AP after the first time the rogue is scanned. By entering the transient interval, you can control the time interval at which the AP should scan for rogues. The APs can filter the rogues based on their transient

interval values. Valid range is between 120 seconds to 1800 seconds, and the default value is 0. This feature is applicable to APs that are in monitor mode only.

- Rogue Clients
  - Validate rogue clients against AAA—Select the check box to use the AAA server or local database to validate if rogue clients are valid clients. The default value is unselected.
  - Detect and report Adhoc networks—Select the check box to enable ad-hoc rogue detection and reporting. The default value is selected.

View Rogue AP Policies on Controllers, on page 104
Configure Client Exclusion Policies on Controllers, on page 104
View Cisco-Supplied IDS Signatures Applied to Controllers, on page 105
Create Custom IDS Signatures, on page 109
Configure a Controller's AP Authentication and Management Frame Protection , on page 110
Configure Wireless Protection Policies on Controllers , on page 102

View Rogue AP Policies on Controllers

This page enables you to view and edit current Rogue AP Rules.

To access the Rogue AP Rules page, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **Wireless Protection Policies** > **Rogue AP Rules**. The Rogue AP Rules displays the Rogue AP Rules, the rule types (Malicious or Friendly), and the rule sequence.

Step 4 Click a Rogue AP Rule to view or edit its details.

Configure Client Exclusion Policies on Controllers, on page 104
View Cisco-Supplied IDS Signatures Applied to Controllers, on page 105
Create Custom IDS Signatures, on page 109
Configure a Controller's AP Authentication and Management Frame Protection , on page 110
Configure Wireless Protection Policies on Controllers , on page 102

Configure Client Exclusion Policies on Controllers

This page enables you to set, enable, or disable the client exclusion policies applied to the controller.

To access the Client Exclusion Policies page, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > Wireless Protection Policies > Client Exclusion Policies**. The following parameters appear:

- Excessive 802.11a Association Failures—If enabled, clients are excluded on the sixth 802.11 association attempt, after five consecutive failures.
- Excessive 802.11a Authentication Failures—If enabled, clients are excluded on the sixth 802.11 authentication attempt, after five consecutive failures.
- Excessive 802.11x Authentication Failures—If enabled, clients are excluded on the fourth 802.1X authentication attempt, after three consecutive failures.
- Excessive 802.11 Web Authentication Failures—If enabled, clients are excluded on the fourth web authentication attempt, after three consecutive failures.
- IP Theft Or Reuse—If enabled, clients are excluded if the IP address is already assigned to another device.

Step 4 Click **Save** to save the changes made to the client exclusion policies and return to the previous page or click **Audit** to compare Prime Infrastructure values with those used on the controller.

View Rogue AP Policies on Controllers, on page 104
View Cisco-Supplied IDS Signatures Applied to Controllers, on page 105
Create Custom IDS Signatures, on page 109
Configure a Controller's AP Authentication and Management Frame Protection , on page 110
Configure Wireless Protection Policies on Controllers , on page 102

Configure a Device's IDS Signatures

You can configure IDS Signatures, or bit-pattern matching rules used to identify various types of attacks in incoming 802.11 packets, on the controller. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller. If an attack is detected, an appropriate mitigation action is initiated.

Cisco supports 17 standard signatures on controllers.

View Cisco-Supplied IDS Signatures Applied to Controllers, on page 105
Create Custom IDS Signatures, on page 109
Configure a Controller's AP Authentication and Management Frame Protection , on page 110

View Cisco-Supplied IDS Signatures Applied to Controllers

The Standard Signature Parameters page shows the list of Cisco-supplied signatures that are currently on the controller.

To access the Standard Signatures page, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **Wireless Protection Policies** > **Standard Signatures**. This page displays the following parameters:

- Precedence—The order in which the controller performs the signature checks.
- Name—The type of attack the signature is trying to detect.
- Frame Type—Management or data frame type on which the signature is looking for a security attack.
- Action—What the controller is directed to do when the signature detects an attack. For example:
  - None—No action is taken.
  - Report—Report the detection.
- State—Enabled or Disabled.
- Description—A more detailed description of the type of attack the signature is trying to detect.

Step 4 Click a signature name to view individual parameters and to enable or disable the signature.

Related Topics

Configure a Device's IDS Signatures, on page 105
Upload IDS Signature Files From Controllers, on page 107
Enabling and Disabling All IDS Signatures on a Controller, on page 107

Download IDS Signature Files to Controllers

To download a signature file, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **Wireless Protection Policies** > **Standard Signatures** or **Security** > **Wireless Protection Policies** > **Custom Signatures**.

Step 4 From the Select a command drop-down list, choose **Download Signature Files**.

Step 5 Click **Go**.

Step 6 Copy the signature file (*.sig) to the default directory on your TFTP server.

Step 7 Choose **Local Machine** from the File is Located On. If you know the filename and path relative to the server root directory, you can also choose **TFTP server**.

Step 8 Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries.

Step 9 Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout.

Step 10 The signature files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click **Browse** to navigate to it. A “revision” line in the signature file specifies whether the file is a Cisco-provided standard signature file or a site-tailored custom signature file (custom signature files must always have revision=custom).

If the transfer times out for some reason, choose the TFTP server option in the File Is Located On field, and the server filename is populated for you and retried. The local machine option initiates a two-step operation. First, the local file is copied from the administrator workstation to Prime Infrastructure own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in Prime Infrastructure server TFTP directory, and the downloaded web page now automatically populates the filename.

Step 11 Click **OK**.

Related Topics

Configure a Device's IDS Signatures, on page 105

Upload IDS Signature Files From Controllers

You can upload a signature file from controllers. Make sure you have a Trivial File Transfer Protocol (TFTP) server available for the signature download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port cannot be routed.
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port cannot be routed.
- A third-party TFTP server cannot run on the same computer as Prime Infrastructure because Prime Infrastructure built-in TFTP server and third-party TFTP server use the same communication port:

Step 1 Obtain a signature file from Cisco (*standard* signature file).

Step 2 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 3 Click the device name of the applicable controller.

Step 4 From the left sidebar menu, choose **Security** > **Wireless Protection Policies** > **Standard Signatures** or **Security** > **Wireless Protection Policies** > **Custom Signatures**.

Step 5 From the Select a command drop-down list, choose **Upload Signature Files from controller**.

Step 6 Specify the TFTP server name being used for the transfer.

Step 7 If the TFTP server is new, enter the TFTP IP address in the **Server IP Address** field.

Step 8 Choose **Signature Files** from the File Type drop-down list.

The signature files are uploaded to the root directory which was configured for use by the TFTP server. You can change to a different directory at the Upload to File field (this field only shows if the Server Name is the default server). The controller uses this local filename as a base name and then adds _std.sig as a suffix for standard signature files and _custom.sig as a suffix for custom signature files.

Step 9 Click **OK**.

Configure a Device's IDS Signatures, on page 105
Download IDS Signatures to Controllers, on page 10

Enabling and Disabling All IDS Signatures on a Controller

This command enables all signatures that were individually selected as enabled. If this text box remains unselected, all files are disabled, even those that were previously enabled. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller.

To enable all standard and custom signatures currently on the controller, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the Select a command drop-down list, choose **Edit Signature Parameters**.

Step 4 Click **Go**.

Step 5 Select the **Enable Check for All Standard and Custom Signatures** check box.

Step 6 Click **Save**.

Configure a Device's IDS Signatures, on page 105

Enabling and Disabling Single IDS Signatures on a Controller

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the Select a command drop-down list, choose **Edit Signature Parameters**.

Step 4 Click an applicable Name for the type of attack you want to enable or disable.

The Standard Signature parameters page shows the list of Cisco-supplied signatures that are currently on the controller. The Custom Signatures page shows the list of customer-supplied signatures that are currently on the controller. The following parameters are displayed in both the signature page and the detailed signature page:

- Precedence—The order, or precedence, in which the controller performs the signature checks.
- Name—The type of attack the signature is trying to detect.
- Description—A more detailed description of the type of attack that the signature is trying to detect.
- Frame Type—Management or data frame type on which the signature is looking for a security attack.
- Action—What the controller is directed to do when the signature detects an attack. One possibility is *None* , where no action is taken, and another is Report, to report the detection.
- Frequency—The signature frequency or the number of matching packets per interval that must be identified at the detecting access point level before an attack is detected. The range is 1 to 32,000 packets per interval and the default value is 50 packets per interval.
- Quiet Time—The length of time (in seconds) after which no attacks have been detected at the individual access point level, and the alarm can stop. This time appears only if the MAC information is all or both. The range is 60 to 32,000 seconds and the default value is 300 seconds.
- MAC Information—Whether the signature is to be tracked per network or per MAC address or both at the detecting access point level.
- MAC Frequency—The signature MAC frequency or the number of matching packets per interval that must be identified at the controller level before an attack is detected. The range is 1 to 32,000 packets per interval and the default value is 30 packets per interval.
- Interval—Enter the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval. The range is 1 to 3600 seconds and the default value is 1 second.

- Enable—Select this check box to enable this signature to detect security attacks or unselect it to disable this signature.
- Signature Patterns—The pattern that is being used to detect a security attack.

Step 5 From the Enable drop-down list, choose **Yes**. Because you are downloading a customized signature, you should enable the files named with the _custom.sgi and disable the standard signature with the same name but differing suffix. For example, if you are customizing broadcast probe flood, you want to disable broadcast probe flood in the standard signatures but enable it in custom signatures.

Step 6 Click **Save**.

Configure a Device's IDS Signatures, on page 105
Configure Rogue AP Policies on Controllers, on page 103
View Rogue AP Policies on Controllers, on page 104
Create Custom IDS Signatures, on page 109
Configure Client Exclusion Policies on Controllers, on page 104
Configure a Controller's AP Authentication and Management Frame Protection , on page 110

Create Custom IDS Signatures

The Custom Signature page shows the list of customer-supplied signatures that are currently on the controller.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security** > **Wireless Protection Policies** > **Custom Signatures**. This page displays the following parameters:

- Precedence—The order in which the controller performs the signature checks.
- Name—The type of attack the signature is trying to detect.
- Frame Type—Management or data frame type on which the signature is looking for a security attack.
- Action—What the controller is directed to do when the signature detects an attack. For example:
  - None—No action is taken.
  - Report—Report the detection.
- State—Enabled or Disabled.
- Description—A more detailed description of the type of attack the signature is trying to detect.

Step 4 Click a signature Name to view individual parameters and to enable or disable the signature.

Configure a Device's IDS Signatures, on page 105
Configure Rogue AP Policies on Controllers, on page 103
View Rogue AP Policies on Controllers, on page 104
Configure a Controller's AP Authentication and Management Frame Protection , on page 110

Configure a Controller's AP Authentication and Management Frame Protection

You can set the access point authentication policy and Management Frame Protection (MFP).

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > Wireless Protection Policies > AP Authentication and MFP**.

This page displays the following fields:

- RF Network Name—Not an editable text box. The RF Network Name entered in the General parameters page is displayed here.
- Protection Type—From the drop-down list, choose one of the following authentication policies:
  - **None**—No access point authentication policy.
  - **AP Authentication**—Apply authentication policy.
  - **MFP**—Apply Management Frame Protection.
  - Alarm Trigger Threshold—(Appears only when AP Authentication is selected as the Protection Type). Set the number of hits to be ignored from an alien access point before raising an alarm.

The valid range is from 1 to 255. The default value is 255.

Configure a Device's IDS Signatures, on page 105
Configure Rogue AP Policies on Controllers, on page 103
View Rogue AP Policies on Controllers, on page 104
Create Custom IDS Signatures, on page 109
View Cisco-Supplied IDS Signatures Applied to Controllers, on page 105

URL ACL Configuration

URL filtering feature allows you to control access to Internet websites. It does so by permitting or denying access to specific websites based on information contained in a URL access control list (ACL). The URL filtering then restricts access based on the ACL list.

Using location based filtering, APs are grouped under various AP groups and WLAN profiles separate trusted and non-trusted clients within the same SSID. This forces re-authentication and new VLAN when a trusted client moves to a non-trusted AP or vice-versa.

The Wireless Controller (WLC) supports up to 64 ACLs and each ACL can contain up to 100 URLs. These ACLs are configured to either allow or deny requests, and can be associated with different interfaces (ex: WLAN, LAN), thus increasing effective filtering. Policies can be implemented locally on a WLAN or an AP group that is different from the applied global policy.

The number of rules (URLs) supported in each ACL varies for different WLCs:

- Cisco 5508 WLC and WiSM2 support 64 rules in per URL ACL.
- Cisco 5520, 8510, and 8540 WLCs support 100 rules per URL ACL.

Restrictions for URL Filtering and NAT

- Not supported on Cisco 2504 WLCs, vWLC, and Mobility Express.
- Supports WLAN Central Switching and not Local switching.
- Not supported in Flex mode with local switching.
- URL name is limited to 32 characters in length.
- No AVC Profile for the matched URLs. ACL Actions support for the Matched URLs.
- Allowed list and Blocked list can be created using the "*" implicit rule in the ACL to allow or deny requests respectively.
- HTTPS URLs are not supported.
- ACL may fail to filter in the following situations:
  - URL is across fragmented packets.
  - IP packets are fragmented.
  - Direct IP address or proxy setup used instead of URL
- These are currently not supported. If any URL matches with these conditions, it will not be considered for filtering.
  - Wildcard URLs (ex: www.uresour*loc.com)
  - Sub-URL (ex: www.uresour*loc.com/support)
  - Sub-Domain (ex: reach.url.com or sub1.url.com)
- If there is any duplicate URL present while creating the template, then the duplicate URL Rule is not considered

Configure a Access Control List

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > URL ACLs.

This page displays the following fields:

- Checkbox—Use the check box to select one or more URL ACLs to delete.
- URL ACL Name—User-defined name of this template. Click the URL ACL item to view the description.

Step 4 Click an URL ACL.

Step 5 Under Rules, click Add Row to add URL ACL rules.

- In the URL text box, enter the name for the URL ACLs.
- From the Rule Action, drop-down list, select Allow or Deny from the drop-down list.

Step 6 Click Save.

Configure Security Settings for a Controller or Device, on page 83
Delete an URL ACL, on page 112

Delete an URL ACL

To delete an URL ACL, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click a controller Device Name.

Step 3 From the left sidebar menu, choose **Security** > **URL ACLs**.

Step 4 From the URL ACLs page, select one or more URL ACLs to delete.

Step 5 From the **Select a command** drop-down list, choose **Delete URL ACLs**.

Step 6 Click **Go**.

Note If you want to clear the counters for an ACL, from the select a command drop-down list, choose Clear Counters.

Related Topics

Configure a Access Control List, on page 111

Flexible Radio Assignment

Flexible Radio Assignment (FRA) is a new core algorithm added to Radio Resource Management (RRM) to analyze the NDP measurements and manage the hardware used to determine the role of the new Flexible Radio (2.4 GHz, 5 GHz, or Monitor) on Cisco Aironet 2800 and 3800 Series Access Points.

The FRA feature allows for either manual configuration of capable APs or for these APs to intelligently determine the operating role of the integrated radios based on the available RF environment. APs with flexible radio can automatically detect when a high number of devices are connected to a network and changes the dual radios in the access point from 2.4 GHz/5 GHz to 5 GHz/5 GHz to serve more clients. The AP performs this task while still monitoring the network for security threats and RF Interference that affects performance. FRA improves mobile user experience for high-density networks. This feature also reduces 2.4-GHz cell congestion by marking some of the 2.4GHz radios as redundant and switching them to 5GHz (client-serving role) or monitor role (2.4GHz and 5GHz). Use the CLI or GUI to configure the radio role.

An AP with flexible radio can operate in the following modes:

- Default operating mode—One radio serves clients in 2.4 GHz mode, while the other serves clients in 5 GHz mode.
- Dual 5 GHz Mode—Both radios operate in the 5 GHz band, actively serving clients to maximize the benefits of 802.11ac Wave 2 and to increase client device capacity.
- Wireless Security Monitoring—One radio serves 5 GHz clients and the other radio scans both 2.4 GHz and 5 GHz bands for wIPS attackers, CleanAir interferers, and rogue devices.

Configure Flexible Radio Assignment

Procedure

	Command or Action	Purpose
Step 1	Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.	
Step 2	Click the device name of the applicable controller.	

Step 3	From the left sidebar menu, choose **802.11** > **Flexible Radio Assignment**. Configure the following in the Flexible Radio Assignment page:
	• Flexible Radio Assignment—The FRA feature is disabled by default. Check the check box to enable FRA and configure the following parameters.
	• Sensitivity—Adjust the FRA sensitivity threshold. This sets the percentage of COF required o consider a radio as redundant. Supported values are:
	  • Low
	  • Medium
	  • High
	• Interval—Set the FRA run interval. Valid range is 1 hour to 24 hours. Default setting is 1 hour. FRA depends on DCA and hence the FRA interval cannot be lesser than the DCA interval.	

Configure a Device's 802.11 Parameters

This section describes the following sections:

- Set Multiple Country Codes on 802.11 Controllers
- Specify When Controllers Cannot Accept More Client Associations (AP Load Balancing)
- Enable Band Selection to Reduce AP Channel Interference
- Ensure IP Multicast Delivery Using MediaStream
- Create RF Profiles That Can Be Used by AP Groups

Set Multiple Country Codes on 802.11 Controllers

To set multiple country support for a single controller that is not part of a mobility group, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 Choose **802.11** > **General** from the left sidebar menu.

Step 4 Select the check box to choose which country you want to add. Access points are designed for use in many countries with varying regulatory requirements. You can configure a country code to ensure that it complies with your country regulations.

Access points might not operate properly if they are not designed for use in your country of operation. For example, an access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Australia. Always be sure to purchase access points that match your country regulatory domain. For a complete list of country codes supported per product, see the following URL: http://www.cisco.com/warp/public/779/smbiz/wireless/approvals.html .

Step 5 Enter the time (in seconds) after which the authentication response times out.

Step 6 Click **Save**.

Related Topics

Specify When Controllers Cannot Accept More Client Associations (AP Load Balancing), on page 114
Enable Band Selection to Reduce AP Channel Interference, on page 115
Ensure IP Multicast Delivery Using MediaStream, on page 117
Create RF Profiles That Can Be Used by AP Groups, on page 118

Specify When Controllers Cannot Accept More Client Associations (AP Load Balancing)

Enabling aggressive load balancing on the controller allows lightweight access points to load balance the wireless clients across access points. Clients are load balanced between the access points on the same controller. Load balancing does not occur between access points on different controllers.

When a wireless client attempts to associate to a lightweight access point, association response packets are sent to the client with an 802.11 response packet including status code 17. This code indicates whether the access point can accept any more associations. If the access point is too busy, the client attempts to associate to a different access point in the area. The system determines if an access point is relatively more busy than its neighbor access points that are also accessible to the client.

For example, if the number of clients on AP1 is more than the number of clients on AP2 plus the load-balancing window, then AP1 is considered to be busier than AP2. When a client attempts to associate to AP1, it receives an 802.11 response packet with status code 17, indicating that the access point is busy, and the client attempts to associate to a different access point.

You can configure the controller to deny client associations up to 10 times (if a client attempted to associate 11 times, it is allowed to associate on the 11th try). You can also enable or disable load balancing on a particular WLAN, which is useful if you want to disable load balancing for a select group of clients (such as time-sensitive voice clients).

To configure aggressive load balancing, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**

Step 2 Click the device name of the applicable controller.

Step 3 Choose **802.11** > **Load Balancing** from the left sidebar menu. The Load Balancing page appears.

Step 4 Enter a value between 1 and 20 for the client window size. The page size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

load-balancing page + client associations on AP with lightest load = load-balancing threshold

In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client page size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.

Step 5 Enter a value between 0 and 10 for the max denial count. The denial count sets the maximum number of association denials during load balancing.

Step 6 Click **Save**.

Step 7 To enable or disable aggressive load balancing on specific WLANs, browse to the WLAN Configuration page, and click the **Advanced** tab. For instructions on using the WLAN Configuration page, see Configuring Controller WLANs in Related Topics.

Related Topics

Set Multiple Country Codes on 802.11 Controllers, on page 113
Enable Band Selection to Reduce AP Channel Interference, on page 115
Ensure IP Multicast Delivery Using MediaStream, on page 117
Create RF Profiles That Can Be Used by AP Groups, on page 118
Create WLANs on a Controller, on page 56

Enable Band Selection to Reduce AP Channel Interference

Band selection enables client radios that are capable of dual-band (2.4- and 5-GHz) operation to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of three non-overlapping channels. To combat these sources of interference and improve overall network performance, you can configure band selection on the controller.

Band selection works by regulating probe responses to clients. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels.

You can enable band selection globally on a controller, or you can enable or disable band selection for a particular WLAN, which is useful if you want to disable it for a select group of clients (such as time-sensitive voice clients).

Band-selection-enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.

Guidelines for Using Band Selection

Follow these guidelines when using band selection:

- Band selection can be used only with Cisco Aironet 1140 and 1250 series access points.
- Band selection operates only on access points that are connected to a controller. A FlexConnect access point without a controller connection does not perform band selection after a reboot.
- The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.

- You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.

To configure band selection:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 Choose **802.11** > **Band Select** from the left sidebar menu. The Band Select page appears.

Step 4 Enter a value between 1 and 10 for the probe cycle count. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

Step 5 Enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle. The default cycle threshold is 200 milliseconds.

Step 6 Enter a value between 10 and 200 seconds for the age out suppression field. Age-out suppression sets the expiration time for pruning previously known 802.11b/g clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 7 Enter a value between 10 and 300 seconds for the age out dual band field. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 8 Enter a value between –20 and –90 dBm for the acceptable client RSSI field. This field sets the minimum RSSI for a client to respond to a probe. The default value is –80 dBm.

Step 9 Click **Save**.

Step 10 To enable or disable band selection on specific WLANs, browse to the WLAN Configuration page and click the **Advanced** tab. For instructions on using the WLAN Configuration page, see Configuring Controller WLANs in Related Topics.

Set Multiple Country Codes on 802.11 Controllers, on page 113
Specify When Controllers Cannot Accept More Client Associations (AP Load Balancing), on page 114
Ensure IP Multicast Delivery Using MediaStream, on page 117
Create RF Profiles That Can Be Used by AP Groups, on page 118
Create WLANs on a Controller, on page 56

Control Priorities for SIP Calls

The Preferred Call feature enables you to specify highest priority to SIP calls made to some specific numbers. The high priority is achieved by allocating bandwidth to such preferred SIP Calls even when there is no available voice bandwidth in the configured Voice Pool. This feature is supported only for those clients that use SIP based CAC for bandwidth allocation in WCS or WLC.

You can configure up to 6 numbers per controller.

To configure the preferred call support, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **802.11** > **Preferred Call**. The following fields appear if there is an existing preferred call:

- Description—Description for the preferred call.
- Number Id—Indicates the unique identifier for the controller and denotes one of the six preferred call numbers assigned to the controller.
- Preferred Number—Indicates the preferred call number.

Step 4 From the Select a command drop-down list, choose **Add Number**.

Step 5 Select a template to apply to this controller.

You need to select a template to apply to the selected controller. To create a New Template for Preferred Call Numbers, see Configuring Preferred Call Templates in Related Topics.

Step 6 Click **Apply**.

To delete a preferred call, select the check box for the applicable preferred call number and choose **Delete** from the Select a command drop-down list. Click **Go** and then click **OK** to confirm the deletion.

Related Topics

Set Multiple Country Codes on 802.11 Controllers, on page 113
Specify When Controllers Cannot Accept More Client Associations (AP Load Balancing), on page 114
Enable Band Selection to Reduce AP Channel Interference, on page 115
Create RF Profiles That Can Be Used by AP Groups, on page 118

Ensure IP Multicast Delivery Using MediaStream

To configure media parameters for 802.11, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **802.11** > **Media Stream**.

Step 4 In the Media Stream Configuration section, configure the following parameters

- Media Stream Name
- Multicast Destination Start IP—Start IP address of the media stream to be multicast
- Multicast Destination End IP—End IP address of the media stream to be multicast
- Maximum Expected Bandwidth—Maximum bandwidth that a media stream can use

Step 5 In the Resource Reservation Control (RRC) Parameters group box, configure the following parameters:

- Average Packet Size—Average packet size that a media stream can use.
- RRC Periodical Update—Resource Reservation Control calculations that are updated periodically; if disabled, RRC calculations are done only once when a client joins a media stream.
- RRC Priority—Priority of RRC with the highest at 1 and the lowest at 8.

- Traffic Profile Violation—Appears if the stream is dropped or put in the best effort queue if the stream violates the QoS video profile.
- Policy—Appears if the media stream is admitted or denied.

Step 6 Click **Save**.

Create RF Profiles That Can Be Used by AP Groups

The RF Profiles page enables you to create or modify RF profiles that get associated to AP Groups.

To configure a RF Profile for a controller, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 Click **RF Profiles** or choose either **802.11 > RF Profiles** from the left sidebar menu. The RF Profiles page appears. This page lists the existing RF Profile templates.

Step 4 If you want to add a RF profile, choose **Add RF Profile** from the Select a command drop-down list.

Step 5 Click **Go**. The New Controller Template page appears.

Step 6 Configure the following information:

- General
  - Template Name—User-defined name for the template. Profile Name—User-defined name for the current profile. Description—Description of the template.
  - Radio Type—The radio type of the access point. This is a drop-down list from which you can choose an RF profile for APs with 802.11a or 802.11b radios.
- TCP (Transmit Power Control)
  - Minimum Power Level Assignment (-10 to 30 dBm)—Indicates the minimum power assigned. The range is -10 to 30 dB, and the default value is 30 dB.
  - Maximum Power Level Assignment (-10 to 30 dBm)—Indicates the maximum power assigned. The range is -10 to 30 dB, and the default value is 30 dB.
  - Power Threshold v1(-80 to -50 dBm)—Indicates the transmitted power threshold. Power Threshold v2(-80 to -50 dBm)—Indicates the transmitted power threshold.
- Data Rates—Use the Data Rates drop-down lists to specify the rates at which data can be transmitted between the access point and the client. These data rates are available:
  - 802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps.
  - 802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps.

  For each data rate, choose one of these options:

  - Mandatory—Clients must support this data rate to associate to an access point on the controller.
  - Supported—Any associated clients that support this data rate might communicate with the access point using that rate. However, the clients are not required to be able to use this rate to associate.
  - Disabled—The clients specify the data rates used for communication.

Step 7 Click **Save**.

Related Topics

Set Multiple Country Codes on 802.11 Controllers, on page 113
Specify When Controllers Cannot Accept More Client Associations (AP Load Balancing), on page 114
Enable Band Selection to Reduce AP Channel Interference, on page 115

Configure a Device's 802.11a/n Parameters

To view 802.11a/n parameters for a specific controller, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller.**

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose one of the following:

- **802.11a/n > Parameters** to view or edit the parameters.
- **802.11a or n or ac > dot11a-RRM > RRM Thresholds** to configure the 802.11a/n RRM threshold controller.
- **802.11a/n > RRM Intervals** or **802.11b/g/n > RRM Intervals** to configure the 802.11a/n or 802.11b/g/n RRM intervals for an individual controller.
- **802.11a/n-RRM > TPC** to configure the 802.11a/n or 802.11b/g/n RRM Transmit Power Control.
- **802.11a or n or ac >dot11a-RRM > DCA** to configure the RRM Dynamic Channel Allocation.
- **802.11a/n > RRM > RF Grouping** to configure the 802.11a/n or 802.11b/g/n RRM Radio Grouping for an individual controller.
- **802.11a/n > Media Parameters** to configure the media parameters for 802.11a/n.
- **802.11a/n > EDCA Parameters** or **802.11b/g/n > EDCA** to configure the 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller.
- **802.11a/n > Roaming Parameters** to configure the 802.11a/n or 802.11b/g/n roaming parameters.
- **802.11a/n > 802.11h** or **802.11b/g/n > 802.11h** to configure the 802.11h parameters for an individual controller.
- **802.11a/n > High Throughput** or **802.11b/g/n > High Throughput** to configure the 802.11a/n or 802.11b/g/n high throughput parameters.
- **802.11a/n > CleanAir** to configure 802.11a/n CleanAir parameters.

Step 4 Click Save.

Configure a Device's 802.11b/g/n Parameters

To view 802.11b/g/n parameters for a specific controller, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller.**

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose one of the following:

- **802.11b/g/n Parameters** to view or edit the parameters.
- **802.11b or g or n > dot11b-RRM > Thresholds** to configure the 802.11b/g/n RRM Thresholds.
- **802.11a/n > RRM Intervals** or **802.11b/g/n > RRM Intervals** to configure the 802.11b/g/n RRM Intervals.
- **802.11b/g/n-RRM > TPC** to configure the 802.11b/g/n RRM Transmit Power Control parameters.
- **802.11b or g or n > dot11b-RRM > DCA** to configure the 802.11a/n or 802.11b/g/n RRM DCA channels for an individual controller
- **802.11b/g/n > RRM > RF Grouping** to configure the 802.11a/n or 802.11b/g/n RRM Radio Grouping for an individual controller.
- **802.11b/g/n > Media Parameters** to configure the media parameters for 802.11b/g/n.
- **802.11a/n > EDCA Parameters** or **802.11b/g/n > EDCA** to configure the 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller.
- **802.11a/n > Roaming Parameters** or **802.11b/g/n > Roaming Parameters** to configure the 802.11a/n or 802.11b/g/n EDCA parameters.
- **802.11a/n > High Throughput** or **802.11b/g/n > High Throughput** to configure the 802.11a/n or 802.11b/g/n high throughput parameters.
- **802.11b/g/n > CleanAir** to configure the 802.11b/g/n CleanAir parameters

Step 4 Click Save.

Configure a Device's Mesh Parameters

To configure Mesh parameters for an individual controller, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Mesh** > **Mesh Settings**.

Step 4 View or edit the following mesh parameters:

- RootAP to MeshAP Range —By default, this value is 12,000 feet. You can enter a value between 150 and 132,000 feet. Enter the optimum distance (in feet) that exists between the root access point and the mesh access point. This global field applies to all access points when they join the controller and all existing access points in the network.
- Client Access on Backhaul Link—Enabling this feature lets mesh access points associate with 802.11a wireless clients over the 802.11a backhaul. This is in addition to the existing communication on the 802.11a backhaul between

the root and mesh access points. This feature is applicable only to the access points with two radios. Changing Backhaul Client Access reboots all the mesh access points. See the “Client Access on 1524SB Dual Backhaul” in the Related Topics for more information.

The Mesh Background Scanning and Auto parent selection feature enables a mesh access point (MAP) to find and connect with a better potential parent across channels and maintain its uplink with the best parent all the time.

This feature eliminates the time consuming task of finding a parent across channels by scanning all the channels. The off-channel procedure transmits broadcast packets on selected channels (at a periodicity of 3 seconds, with a maximum of 50 milliseconds per off-channel) and receives packets from all 'reachable' neighbors. This keeps the child MAP updated with neighbor information across channels enabling it to 'switch' to a new neighbor and use it as a parent for the uplink. The 'switch' need not be triggered from parent loss detection, but on identifying a better parent while the child MAP still has its current parent uplink active.

- Background Scanning—Select the **Background Scanning** check box to enable mesh background scanning feature. The default value is disabled.
- Mesh DCA Channels— Enabling this option lets the backhaul channel to deselect on the controller using the DCA channel list. Any change to the channels in the Controller DCA list is pushed to the associated access points. This option is only applicable for 1524SB mesh access points. See “Backhaul Channel Deselection on Controllers” in the Related Topics for more information.
- Mesh RAP Downlink Backhaul—Changing backhaul downlink slot reboots all Mesh APs.
- Outdoor Access For UNII 1 Band Channels
- Global Public Safety— Enabling this option indicates that 4.9 Ghz can be used on backhaul link by selecting channel on the 802.11a backhaul radio. 4.9Ghz considered to be public safety band and is limited to some service providers. This setting applies at the controller level.
- Security Mode—Choose **EAP** (Extensible Authentication Protocol) or **PSK** (Pre-Shared Key) from the Security Mode drop-down list. Changing Security reboots all mesh access points.

Step 5 Click **Save**.

Related Topics

Enable Client Access to Backhaul Radios on 1524 SB APs, on page 121
Enable Backhaul Channel Deselection on Controllers, on page 122

Enable Client Access to Backhaul Radios on 1524 SB APs

The 1524 Serial Backhaul (SB) access point consists of three radio slots.

- Radio in slot-0 operates in 2.4 GHz frequency band and is used for client access.
- Radios in slot-1 and slot-2 operate in 5.8 GHz band and are primarily used for backhaul.

The two 802.11a backhaul radios use the same MAC address. There might be instances where the same WLAN maps to the same BSSID in more than one slot.

By default, client access is disabled over both the backhaul radios.

These guidelines must be followed to enable or disable a radio slot:

- You can enable client access on slot-1 even if client access on slot-2 is disabled.
- You can enable client access on slot-2 only when client access on slot-1 is enabled.
- If you disable client access on slot-1, then client access on slot-2 is automatically disabled.
- All the Mesh Access Points reboot whenever the client access is enabled or disabled.

The Universal Client Access feature allows client access over both the slot-1 and slot-2 radios. You can configure client access over backhaul radio from either one of the following:

- The Controller command-line interface (CLI)
- The Controller Graphical User Interface (GUI)
- Prime Infrastructure GUI.

To configure client access on the two backhaul radios, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Mesh** > **Mesh Settings**.

Step 4 Select the **Client Access on Backhaul Link** check box.

Step 5 Select the **Extended Backhaul Client Access** check box.

Step 6 Click **Save**.

A warning message is displayed:

Example:

```
Enabling client access on both backhaul slots will use same BSSIDs on both the slots. Changing Backhaul
 Client Access will reboot all Mesh APs.
```

Step 7 Click **OK**.

The Universal Client access is configured on both the radios.

Related Topics

Enable Backhaul Channel Deselection on Controllers, on page 122
Configure a Device's Mesh Parameters , on page 120

Enable Backhaul Channel Deselection on Controllers

To configure backhaul channel deselection, follow these steps:

Step 1 Configure the Mesh DCA channels flag on the controllers. See “Enable Client Access to Backhaul Radios on 1524 SB APs” in Related Topics.

Step 2 Change the channel list using configuration groups. See “Change the Controller Channel List Using Prime Infrastructure Configuration Groups” in Related Topics.

Related Topics

Enable Client Access to Backhaul Radios on 1524 SB APs, on page 121
Configure a Device's Mesh Parameters , on page 120
Change the Controller Channel List Using Cisco Prime Infrastructure Configuration Groups, on page 123

Push Channel Changes from Controllers to 1524 SB APs

You can configure the Mesh DCA Channel flag to push each channel change on one or more controllers to all the associated 1524SB access points. To configure this feature, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Mesh** > **Mesh Settings**.

Step 4 Select the **Mesh DCA Channels** check box to enable channel selection. This option is unselected by default.

The channel changes in the controllers are pushed to the associated 1524SB access points.

Change the Controller Channel List Using Cisco Prime Infrastructure Configuration Groups

You can use controller configuration groups to configure backhaul channel deselection. You can create a configuration group and add the required controllers to the group and use the Country/DCA tab to select or deselect channels for the controllers in that group.

To configure backhaul channel deselection using configuration groups, follow these steps:

Step 1 Choose **Configuration > Controller Configuration Groups**.

Step 2 Select a configuration group to view its configuration group details.

Step 3 From the Configuration Group detail page, click the **Country/DCA** tab.

Step 4 Select or unselect the Update Country/DCA check box.

Related Topics

Enable Client Access to Backhaul Radios on 1524 SB APs, on page 121
Enable Backhaul Channel Deselection on Controllers, on page 122
Configure a Device's Mesh Parameters , on page 120
Push Channel Changes from Controllers to 1524 SB APs, on page 123

Configure a Device's Port Parameters

To configure Port parameters for an individual controller, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices**, then select **Device Type > Wireless Controller**.

Step 2 Click an applicable device.

Step 3 From the left sidebar menu, choose **Ports > Port Settings**.

Step 4 Click the applicable Port Number to open the Port Settings Details page. The following parameters are displayed:

- General Parameters:
  - Port Number—Read-only.
  - Admin Status—Choose Enabled or Disabled from the drop-down list.

- Physical Mode— Auto Negotiate (Read-only)
- Physical Status— Full Duplex 1000 Mbps (Read-only).
- STP Mode—Choose 802.1D, Fast, or Off.
- Link Traps—Choose Enabled or Disabled.
- Power Over Ethernet
- Multicast Application Mode—Select Enabled or Disabled.
- Port Mode SFP Type— Read-only

- Spanning Tree Protocol Parameters:
  - Priority—The numerical priority number of the ideal switch.
  - Path Cost—A value (typically based on hop count, media bandwidth, or other measures) assigned by the network administrator and used to determine the most favorable path through an internetwork environment (lower the cost, better the path).

Step 5 Click **Save.**

Related Topics

Configure a Device's Mesh Parameters , on page 120
Configure a Controller's Management Parameters , on page 124
Configure a Controller’s IPv6 Neighbor Binding and RA Parameters, on page 133
Configure a Controller’s Proxy Mobile IPv6 (PMIP) Parameters, on page 135
Configure a Controller’s Location Information, on page 131
Configure a Controller’s Multicast DNS (mDNS) Settings, on page 138
Configure a Controller’s Application Visibility and Control (AVC) Parameters, on page 140
Configure a Controller’s NetFlow Settings , on page 141

Configure a Controller's Management Parameters

The following management parameters of the controllers can be configured:

- Trap Receivers
- Trap Control
- Telnet and SSH
- Multiple Syslog servers
- Web Admin
- Local Management Users
- Authentication Priority

Related Topics

Configure Controller Traps, on page 125
Configure Syslog Servers on Controllers, on page 127
Configure Controller Telnet SSH Session Parameters, on page 127
Configure Web Admin Management on a Controller, on page 129
Configure Local Management Users on a Controller, on page 130
Configure Controller Management Authentication Server Priority, on page 130

Configure Trap Receivers for a Controller

The trap receiver parameter can be configured for individual wireless controllers. This parameter can be added / deleted from the wireless controller. A trap receiver can be added by creating a template under Configuration > Features & Technologies.

To configure trap receivers for an individual controller, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Management** > **Trap Receiver**.

Step 4 The following parameters are displayed for current trap receivers:

- Community Name— Name of the trap receiver.
- IP Address—The IP address of the server.
- Admin Status—Status must be enabled for the SNMP traps to be sent to the receiver.

Step 5 Click a receiver Name to access its details.

Step 6 Select the **Admin Status** check box to enable the trap receiver. Unselect the check box to disable the trap receiver.

Step 7 Click **Save**.

Step 8 To delete a receiver / receivers, select the applicable receiver / receivers check-box.

Step 9 From the **Select a command** drop-down list, choose **Delete Receivers**.

Step 10 Click **Go**.

Step 11 Click **OK** in the confirmation message.

Configure Controller Traps

To configure trap control parameters for an individual controller, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Management** > **Trap Control**.

Step 4 The following traps can be enabled for this controller:

- Miscellaneous Traps:
  - SNMP Authentication—The SNMPv2 entity has received a protocol message that is not properly authenticated. When a user who is configured in SNMP V3 mode tries to access the controller with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure. Link (Port) Up/Down—Link changes status from up or down. Multiple Users—Two users login with the same login ID. Spanning Tree—Spanning Tree traps. See the STP specifications for descriptions of individual parameters. Rogue AP—Whenever a rogue AP is detected this trap is sent with its MAC address; For a rogue AP that was detected earlier and it no longer exists, this trap is sent. Config

Save—Notification sent when the controller configuration is modified. RFID Limit Reached Threshold— The maximum permissible value for RFID limit.

- Client Related Traps:
  - 802.11 Association—The associate notification is sent when the client sends an association frame. 802.11 Disassociation—The disassociate notification is sent when the client sends a disassociation frame. 802.11 Deauthentication—The deauthenticate notification is sent when the client sends a deauthentication frame. 802.11 Failed Authentication—The authenticate failure notification is sent when the client sends an authentication frame with a status code other than 'successful'. 802.11 Failed Association—The associate failure notification is sent when the client sends an association frame with a status code other than 'successful'. Excluded—The associate failure notification is sent when a client is excluded. 802.11 Authenticated— The authenticate notification is sent when the client sends an authentication frame with a status code 'successful'. MaxClients Limit Reached Threshold— The maximum permissible number of clients allowed.
- Cisco AP Traps:
  - AP Register—Notification sent when an access point associates or disassociates with the controller. AP Interface Up/Down—Notification sent when access point interface (802.11a or 802.11b/g) status goes up or down.
- Auto RF Profile Traps:
  - Load Profile—Notification sent when Load Profile state changes between PASS and FAIL. Noise Profile—Notification sent when Noise Profile state changes between PASS and FAIL. Interference Profile—Notification sent when Interference Profile state changes between PASS and FAIL. Coverage Profile—Notification sent when Coverage Profile state changes between PASS and FAIL.
- Auto RF Update Traps:
  - Channel Update—Notification sent when access point dynamic channel algorithm is updated. Tx Power Update—Notification sent when access point dynamic transmit power algorithm is updated.
- AAA Traps
  - User Auth Failure—This trap is to inform that a client RADIUS Authentication failure has occurred. RADIUS Server No Response—This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.
- 802.11 Security Traps:
  - WEP Decrypt Error—Notification sent when the controller detects a WEP decrypting error. Signature Attack—Notification sent when a signature attack is detected in the wireless controller that uses RADIUS Authentication.

Step 5 After selecting the applicable parameters, click **Save**.

Related Topics

Configure Trap Receivers for a Controller, on page 125
Configure Syslog Servers on Controllers, on page 127
Configure Controller Telnet SSH Session Parameters, on page 127
Configure Web Admin Management on a Controller, on page 129
Configure Local Management Users on a Controller, on page 130

Configure Controller Management Authentication Server Priority, on page 130

Configure Controller Telnet SSH Session Parameters

To configure Telnet SSH (Secure Shell) parameters for an individual controller, follow these steps:

Step 1 Choose **Configuration** > **> Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Management** > **Telnet SSH**.

The following parameters can be configured:

- Session Timeout—Indicates the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there is no timeout. Might be specified as a number from 0 to 160. The factory default is 5.
- Maximum Sessions—From the drop-down list, choose a value from 0 to 5. This object indicates the number of simultaneous Telnet sessions allowed.
- Allow New Telnet Sessions—Indicates that new Telnet sessions are not allowed on the DS Port when set to no. The factory default value is no. New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the Service port.
- Allow New SSH Sessions—Indicates that new Secure Shell Telnet sessions are not allowed when set to no. The factory default value is yes.

Step 4 After configuring the applicable parameters, click **Save.**

Related Topics

Configure Trap Receivers for a Controller, on page 125
Configure Syslog Servers on Controllers, on page 127
Configure Web Admin Management on a Controller, on page 129
Configure Local Management Users on a Controller, on page 130
Configure Controller Management Authentication Server Priority, on page 130

Configure Syslog Servers on Controllers

For Release 5.0.148.0 controllers or later, you can configure multiple (up to three) syslog servers on the WLAN controller. With each message logged, the controller sends a copy of the message to each configured syslog host, provided the message has severity greater than or equal to the configured syslog filter severity level.

To enable syslogs for an individual controller, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Management** > **Multiple Syslog**.

The applied template is identified:

Syslog Server Address—Indicates the server address of the applicable syslog.

Step 4 Click **Save.**

Step 5 To delete syslog server(s), select the syslog server(s) check-box.

Step 6 From the **Select** a command drop-down list, choose **Delete Syslog Servers**.

Step 7 Click **Go**.

Step 8 Click **OK** in the confirmation message.

Related Topics

Configure Trap Receivers for a Controller, on page 125
Configure Controller Traps, on page 125
Configure Controller Telnet SSH Session Parameters, on page 127
Configure Web Admin Management on a Controller, on page 129
Configure Local Management Users on a Controller, on page 130
Configure Controller Management Authentication Server Priority, on page 130

Configure Network Assurance

To push client related data to a web server periodically, enable Network Assurance along with normal WLC functionality. This data is used as input for the newly introduces Assurance related dashboards. To configure Network Assurance for a controller, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Management** > **Network Assurance**.

Step 4 You can view the applied template and configure the following parameters:

- Publish Data to Assurance Server - Global level field which controls network assurance feature.
- Data Externalization - A data model related setting on the controller. To enable Network Assurance, Data Externalization should be enabled first. A change in Data Externalization field value requires WLC reboot.
- NA Server URL - Server address to which WLC posts client data periodically. Server address can be host based or ip address based. If NA Server URL is host based, then NA Server CA Certificate should be generated on host name. Similarly, if URL is IP address based, then certificate should be generated with IP address.

Step 5 Click **Save**.

Related Topics

Download NA Server CA Certificate to Controllers, on page 16
Generating Self Signed Certificates for Network Assurance , on page 14
Configure Trap Receivers for a Controller, on page 125
Configure Syslog Servers on Controllers, on page 127
Configure Controller Telnet SSH Session Parameters, on page 127

Configure Web Admin Management on a Controller

This section provides instructions for enabling the distribution system port as a web port (using HTTP) or as a secure web port (using HTTPS). You can protect communication with the GUI by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Sockets Layer (SSL) protocol. When you enable HTTPS, the controller generates its own local web administration SSL certificate and automatically applies it to the GUI. You can download an externally generated certificate.

To enable WEB admin parameters for an individual controller, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Management** > **Web Admin**.

The following parameters can be configured:

- WEB Mode—Choose **Enable** or **Disable** from the drop-down list. When enabled, users can access the controller GUI using *http:ip-address*. The default is Disabled. Web mode is not a secure connection.
- Secure Web Mode—Choose **Enable** or **Disable** from the drop-down list. When enabled, users can access the controller GUI using *https://ip-address* . The default is Enabled.
- Certificate Type— The Web Admin certificate must be downloaded.The controller must be rebooted for the new Web Admin certificate to take effect.
  - Download Web Admin Certificate—Click to access the Download Web Admin Certificate to Controller page. See "**Download Web Auth or Web Admin Certificates to a Controller**" for more information.

Download Web Auth or Web Admin Certificates to a Controller

To download a Web Auth or Web Admin Certificate to the controller, follow these steps:

Step 1 Click the **Download Web Admin Certificate** or **Download Web Auth Certificate** link.

Step 2 In the File is located on field, specify Local machine or TFTP server. If the certificate is located on the TFTP server, enter the server filename. If it is located on the local machine, click **Browse** and enter the local filename.

Step 3 Enter the TFTP server name in the **Server Name** text box. The default is the Prime Infrastructure server.

Step 4 Enter the server IP address.

Step 5 In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 6 In the Time Out text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 7 In the Local File Name text box, enter the directory path of the certificate.

Step 8 In the Server File Name text box, enter the name of the certificate.

Step 9 Enter the password in the Certificate Password text box.

Step 10 Re-enter the above password in the Confirm Password text box.

Step 11 Click **OK**.

Step 12 Click **Regenerate Cert** to regenerate the certificate.

Related Topics

Configure Trap Receivers for a Controller, on page 125
Configure Controller Traps, on page 125
Configure Controller Telnet SSH Session Parameters, on page 127
Configure Web Admin Management on a Controller, on page 129
Configure Local Management Users on a Controller, on page 130
Configure Controller Management Authentication Server Priority, on page 130

Configure Local Management Users on a Controller

This page lists the names and access privileges of the local management users. You can also delete the local management user.

To access the Local Management Users page, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Management** > **Local Management Users**.

Step 4 Click a username.

- User Name (read-only)—Name of the user.
- Access Level (read-only)—Read Write or Read Only.

Step 5 To delete the Local Management User, select the user(s) check-box.

Step 6 From the Select a command drop-list, choose Delete Local Management Users.

Step 7 Click Go.

Step 8 Click OK in the confirmation message.

Configure Trap Receivers for a Controller, on page 125
Configure Controller Traps, on page 125
Configure Controller Telnet SSH Session Parameters, on page 127
Configure Web Admin Management on a Controller, on page 129
Configure Controller Management Authentication Server Priority, on page 130

Configure Controller Management Authentication Server Priority

Authentication Priority is configured to control the order in which authentication servers are used to authenticate controller management users.

To access the Authentication Priority page, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Management > Authentication Priority**.

Step 4 The local database is searched first. Choose either RADIUS or TACACS+ for the next search. If authentication using the local database fails, the controller uses the next type of server.

Step 5 Click **Save**.

Related Topics

Configure a Controller's Management Parameters , on page 124
Configure a Device's Mesh Parameters , on page 120
Configure a Device's Port Parameters , on page 123
Configure a Controller's Location Information, on page 131
Configure a Controller's IPv6 Neighbor Binding and RA Parameters, on page 133
Configure a Controller's Proxy Mobile IPv6 (PMIP) Parameters, on page 135
Configure a Controller's Multicast DNS (mDNS) Settings, on page 138
Configure a Controller's Application Visibility and Control (AVC) Parameters, on page 140
Configure a Controller's NetFlow Settings , on page 141

Configure a Controller's Location Information

Currently WiFi clients are moving towards lesser probing to discover an AP. Smartphones do this to conserve battery power. The applications on a smartphone have difficulty generating probe request but can easily generate data packets and hence trigger enhanced location for the application. Hyperlocation is configured from WLC 8.1MR and Prime Infrastructure. It is ultra-precise in locating beacons, inventory, and personal mobile devices. Some networks use multiple access points to get location coordinates within 5 to 7 meters of accuracy, but Hyperlocation can track locations to within a single meter.

To configure location configurations for an individual controller, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **Location > Location Configuration**.

The Location Configuration page displays two tabs: General and Advanced.

Step 4 Add or modify the General parameters:

- RFID Tag Data Collection—Select the check box to enable the collection of data on tags.

Before the location server can collect asset tag data from controllers, you must enable the detection of active RFID tags using the CLI command **config rfid status enable** on the controllers.

- Location Path Loss Configuration
  - Calibrating Client—Select the check box to enable calibration for the client. Controllers send regular S36 or S60 requests (depending on the client capability) by way of the access point to calibrate clients. Packets are

transmitted on all channels. All access points gather RSSI data from the client at each location. These additional transmissions and channel changes might degrade contemporaneous voice or video traffic.

- Normal Client—Select the check box to have a non-calibrating client. No S36 requests are transmitted to the client. S36 is compatible with CCXv2 or later whereas S60 is compatible with CCXv4 or later.

- Measurement Notification Interval (in secs)
  - Tags, Clients, and Rogue APs/Clients—Allows you to set the NMSP measurement notification interval for clients, tags, and rogues. Specify how many seconds should elapse before notification of the found element (tags, clients, and rogue access points/clients).

Setting this value on the controller generates an out-of-sync notification which you can view in the Synchronize Servers page. When different measurement intervals exist between a controller and the mobility services engine, the largest interval setting of the two is adopted by the mobility services engine.

Once this controller is synchronized with the mobility services engine, the new value is set on the mobility services engine. Synchronization to the mobility services engine is required if changes are made to measurement notification interval.

- RSS Expiry Timeout (in secs)
  - For Clients—Enter the number of seconds after which RSSI measurements for normal (non-calibrating) clients must be discarded.
  - For Calibrating Clients—Enter the number of seconds after which RSSI measurements for calibrating clients must be discarded.
  - For Tags—Enter the number of seconds after which RSSI measurements for tags must be discarded.
  - For Rogue APs—Enter the number of seconds after which RSSI measurements for rogue access points must be discarded.

Step 5 Add or modify the Advanced parameters:

- RFID Tag Data Timeout (in secs)—Enter a value (in seconds) to set the RFID tag data timeout setting.
- Location Path Loss Configuration
  - Calibrating Client Multiband—Select the **Enable** check box to send S36 and S60 packets (where applicable) on all channels. Calibrating clients must be enabled in the general tab as well. To use all radios (802.11a/b/g/n) available, you must enable multiband.
- Hyperlocation Config Parameters
  - Hyperlocation— By enabling this option, all the APs associated to that controller which have the Hyperlocation module will be enabled.
  - Packet Detection RSSI Minimum—Adjust this value to filter out weak RSSI readings from location calculation.
  - Scan Count Threshold for Idle Client Detection—The maximum permissible count of the idle clients detected while scanning.
  - NTP Server IP Address—Enter the valid NTP server IP address.This IP address is used by all APs for time synchronization.
  - Azimuth angle — Refer below table for correct Azimuth values:

Table 2: Azimuth Values

Mount Position	Arrow Direction	Azimuth (in Degrees)	Elevation (in Degrees)
Ceiling Mount	South	90	0 (Up)

Mount Position	Arrow Direction	Azimuth (in Degrees)	Elevation (in Degrees)
East Wall Mount	East	0	90 (Down)
South Wall Mount	South	90	90 (Down)
West Wall Mount	West	180	90 (Down)
North Wall Mount	North	270	90 (Down)
Angled North Wall at 45degrees	North	270	45 (Down)

Tip Install the APs on the ceiling grid and if possible, try to align Hyperlocation arrow on AP so they all are pointing in the same direction. The recommendation is to mount APs in default orientation.

Step 6 Click **Save**.

Related Topics

Configure a Controller's Management Parameters , on page 124
Configure a Controller's IPv6 Neighbor Binding and RA Parameters, on page 133
Configure a Controller's Proxy Mobile IPv6 (PMIP) Parameters, on page 135
Configure a Device's Mesh Parameters , on page 120
Configure a Device's Port Parameters , on page 123
Configure a Controller's Multicast DNS (mDNS) Settings, on page 138
Configure a Controller's Application Visibility and Control (AVC) Parameters, on page 140
Configure a Controller's NetFlow Settings , on page 141

Configure a Controller's IPv6 Neighbor Binding and RA Parameters

IPv6 can be configured with Neighbor Binding Timer and Router Advertisements (RA) parameters.

Related Topics

Configure Controller Neighbor Binding Timers, on page 133
Configure Router Advertisement Throttling on Controllers, on page 134
Configure RA Guard on Controllers, on page 134

Configure Controller Neighbor Binding Timers

To configure the Neighbor Binding Timers, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **IPv6** > **Neighbor Binding Timers**.

Step 4 The applied template will be displayed. Add or modify the following parameters:

- Down Lifetime Interval— This indicates the maximum time, in seconds. The range is 0 to 86,400 seconds, and the default value is 0.

- Reachable Lifetime Interval—This indicates the maximum time, in seconds. The range is 0 to 86,400 seconds, and the default value is 0.
- Stale Lifetime Interval—This indicates the maximum time, in seconds. The range is 0 to 86,400 seconds, and the default value is 0.

Step 5 Click **Save**.

Configure Router Advertisement Throttling on Controllers

The RA Throttle Policy allows you to limit the amount of multicast Router Advertisements (RA) circulating on the wireless network.

To configure RA Throttle Policy, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **IPv6** > **RA Throttle Policy**.

Step 4 If you want to enable the RA Throttle Policy, select the **Enable** check box and configure the following parameters:

- Throttle Period—Duration of the throttle period in seconds. The range is 10 to 86,400 seconds.
- Max Through—The number of RA that passes through over a period or over an unlimited period. If the No Limit check-box is not enabled, the maximum pass-through number can be specified.
- Interval Option—Indicates the behavior in case of RA with an interval option.
  - Ignore
  - Passthrough
  - Throttle
- Allow At-least—Indicates the minimum number of RA not throttled per router.
- Allow At-most—Indicates the maximum or unlimited number of RA not throttled per router. If the No Limit check-box is not enabled, the maximum number of RA not throttled per router can be specified.

Step 5 Click **Save**.

Related Topics

Configure Controller Neighbor Binding Timers, on page 133
Configure RA Guard on Controllers, on page 134

Configure RA Guard on Controllers

RA Guard is a Unified Wireless solution to drop RA from wireless clients. It is configured globally, and by default it is enabled. You can configure IPv6 Router Advertisement parameters.

To configure RA Guard, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose **IPv6** > **RA Guard**.

Step 4 If you want to enable the Router Advertisement Guard, select the **Enable** check box.

Step 5 Click **Save**.

Related Topics

Configure Controller Neighbor Binding Timers, on page 133
Configure Router Advertisement Throttling on Controllers, on page 134

Configure a Controller's Proxy Mobile IPv6 (PMIP) Parameters

Proxy Mobile IPv6 is a network-based mobility management protocol that supports a mobile node by acting as the proxy for the mobile node in any IP mobility-related signaling. The mobility entities in the network track the movements of the mobile node and initiate the mobility signaling and set up the required routing state.

The main functional entities are the Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG). The LMA maintains the reachability state of the mobile node and is the topological anchor point for the IP address of the mobile node. The MAG performs the mobility management on behalf of a mobile node. The MAG resides on the access link where the mobile node is anchored. The controller implements the MAG functionality.

Related Topics

Configure PMIP Global Parameters on Controllers, on page 135
Configure PMIP Local Mobility Anchors on Controllers, on page 136
Configure PMIP Profiles on Controllers, on page 137

Configure PMIP Global Parameters on Controllers

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 Choose **PMIP** > **Global Config**from the left sidebar menu.

Step 4 Configure the following fields:

- Domain Name—Read-only.
- MAG Name—Read-only.
- MAG Interface—Read-only.
- Maximum Bindings Allowed—Maximum number of binding updates that the controller can send to the MAG. The valid range is between 0 to 40000.
- Binding Lifetime—Lifetime of the binding entries in the controller. The valid range is between 10 to 65535 seconds. The default value is 65535. The binding lifetime should be a multiple of 4 seconds.

- Binding Refresh Time—Refresh time of the binding entries in the controller. The valid range is between 4 to 65535 seconds. The default value is 300 seconds. The binding refresh time should be a multiple of 4 seconds.
- Binding Initial Retry Timeout—Initial timeout between the proxy binding updates (PBUs) when the controller does not receive the proxy binding acknowledgments (PBAs). The valid range is between 100 to 65535 seconds. The default value is 1000 second.
- Binding Maximum Retry Timeout—Maximum timeout between the proxy binding updates (PBUs) when the controller does not receive the proxy binding acknowledgments (PBAs). The valid range is between 100 to 65535 seconds. The default value is 32000 seconds.
- Replay Protection Timestamp—Maximum amount of time difference between the timestamp in the received proxy binding acknowledgment and the current time of the day. The valid range is between 1 to 255 milliseconds. The default value is 7 milliseconds.
- Minimum BRI Retransmit Timeout—Minimum amount of time that the controller waits before retransmitting the BRI message. The valid range is between 500 to 65535 seconds.
- Maximum BRI Retransmit Timeout—Maximum amount of time that the controller waits before retransmitting the Binding Revocation Indication (BRI) message. The valid range is between 500 to 65535 seconds. The default value is 2000 seconds.
- BRI Retries—Number of BRI retries.
- MAG APN— Name of the Access Point Node of MAG.

Step 5 Click Save.

Related Topics

Configure a Controller's Proxy Mobile IPv6 (PMIP) Parameters, on page 135
Configure PMIP Local Mobility Anchors on Controllers, on page 136
Configure PMIP Profiles on Controllers, on page 137

Configure PMIP Local Mobility Anchors on Controllers

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 Choose **PMIP** > **LMA Config**from the left sidebar menu.

Step 4 Configure the following fields:

- LMA Name—Name of the LMA connected to the controller.
- LMA IP Address—IP address of the LMA connected to the controller.

Step 5 Click **Save**.

Step 6 To delete the LMA configurations, select the applicable LMA config check-box.

Step 7 From the **Select** a command drop-list, choose **Delete PMIP Local Configs**.

Step 8 Click **Go**.

Step 9 Click **OK** in the confirmation message.

Related Topics

Configure PMIP Global Parameters on Controllers, on page 135
Configure PMIP Profiles on Controllers, on page 137
Configure a Controller's Proxy Mobile IPv6 (PMIP) Parameters, on page 135

Configure PMIP Profiles on Controllers

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 Choose **PMIP PMIP Profile** from the left sidebar menu.

Step 4 Enter the profile name.

Step 5 Click **Add** and then configure the following fields:

- Network Access Identifier—Name of the Network Access Identifier (NAI) associated with the profile.
- LMA Name—Name of the LMA to which the profile is associated.
- Access Point Node—Name of the access point node connected to the controller.

Step 6 Click **Save**.

Step 7 To delete the PMIP profiles, select the required PMIP profiles check-box.

Step 8 From the **Select a command** drop-list, choose **Delete PMIP Local Configs**.

Step 9 Click **Go**.

Step 10 Click **OK** in the confirmation message.

Related Topics

Configure PMIP Global Parameters on Controllers, on page 135
Configure PMIP Local Mobility Anchors on Controllers, on page 136
Configure a Controller's Proxy Mobile IPv6 (PMIP) Parameters, on page 135

Configure a Controller's EoGRE Tunneling

Ethernet over GRE (EoGRE) is a solution for aggregating Wi-Fi traffic from hotspots. This solution enables customer-premises equipment (CPE) devices to bridge the Ethernet traffic coming from an end host, and encapsulate the traffic in Ethernet packets over an IP GRE tunnel. When the IP GRE tunnels are terminated on a service provider broadband network gateway, the end host's traffic is terminated and subscriber sessions are initiated for the end host.

To configure EoGRE tunneling, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**. then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 Choose **Tunneling** > **EoGRE** from the left sidebar menu.

Step 4 From the **Interface Name** drop-down list, choose the source interface to tunnel.

Step 5 To create a tunnel gateway:

- Set the **Heartbeat Interval**. The default interval is 60 seconds.
- Set the **Max Heartbeat Skip Count**. The default value is set to 3. If the Tunnel Gateway (TGW) does not reply after three keepalive pings, Cisco WLC marks the TGW as nonoperational. The number of skip count decides how many times the TGW can skip consecutive replies, before the Cisco WLC knows that the TGW is nonoperational.
- Under **Tunnel Gateway**, click **Add Row** and configure tunnel gateway. You can create 10 such gateways.
  a. In the **Tunnel Gateway Name** field, enter the tunnel gateway name.
  b. In the **Tunnel IP Address**field, enter the tunnel IP address. Both IPv4 and IPv6 address formats are supported.
  c. Click **Save**.

     The default tunnel type is EoGRE.
  d. The **Status** can be **UP** or **DOWN** depending on the traps collected.
- Under **Domain**, click **Add Row** and configure the domain (domain is the grouping of two tunnel gateways).
  a. In the**Domain Name** text box, enter the domain name.
  b. From the **Primary Gateway** drop-down list, choose the primary tunnel gateway.
  c. From the **Secondary Gateway** drop-down list, choose the secondary tunnel gateway.

Step 6 Click **Save**.

Configure a Controller's Multicast DNS (mDNS) Settings

Multicast DNS (mDNS) service discovery provides a way to announce and discover services on the local network. mDNS perform DNS queries over IP multicast and supports zero configuration IP networking.

You can configure mDNS so that the controller can learn about the mDNS services and advertise these services to all clients.

There are two tabs in mDNS—Services and Profiles.

- Services tab—This tab enables you to configure the global mDNS parameters and update the Primary Services database.
- Profiles tab—This tab enables to view the mDNS profiles configured on the controller and create new mDNS profiles. After creating a new profile, you must map the profile to an interface group, an interface, or a WLAN. Clients receive service advertisements only for the services associated with the profile. The controller gives the highest priority to the profiles associated to interface groups, followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority. By default, the controller has an mDNS profile, default-mdns-profile which cannot be deleted.

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 Choose **mDNS > mDNS** from the left sidebar menu.

Step 4 On the Services tab, configure the following parameters:

- Template Applied—The name of the template applied to this controller.
- Template Applied—The name of the template applied to this controller.
- Query Interval(10-120)—mDNS query interval, in minutes that you can set. This interval is used by WLC to send periodic mDNS query messages to services which do not send service advertisements automatically after they are started. The range is from 10 to 120 minutes. The default value is 15 minutes.
- rimary Services—Click **Add Row** and then configure the following fields:
  - Primary Service Name—Drop-down list from which you can choose the supported services that can be queried. To add a new service, enter or choose the service name, enter the service string, and then choose the service status. The following services are available

    :
  - AirTunes
  - AirPrint
  - AppleTV
  - HP Photosmart Printer1
  - HP Photosmart Printer2
  - Apple File Sharing Protocol (AFP)
  - Scanner
  - Printer
  - FTP
  - iTunes Music Sharing
  - iTunes Home Sharing
  - iTunes Wireless Device Syncing
  - Apple Remote Desktop
  - Apple CD/DVD Sharing
  - Time Capsule Backup
- Primary Services—Click **Add Row** and then configure the following fields:
- Primary Service Name—Name of the mDNS service.
- Service String—Unique string associated to an mDNS service. For example, _airplay._tcp.local. is the service string associated to AppleTV.
- Query Status—Check box that you select to enable an mDNS query for a service. Periodic mDNS query messages will be sent by WLC at configured Query Interval for services only when the query status is enabled; otherwise, service should automatically advertised for other services where the query status is disabled (for example AppleTV).

Step 5 On the Profiles tab, configure the following parameters:
'

- Profiles—Click **Add Profile** and then configure the following fields:
  - Profile Name—Name of the mDNS profile. You can create a maximum of 16 profiles.
  - Services—Select the services (using the check boxes) that you want to map to the mDNS profile.

Step 6 Click **Save**.

What to do next

By default, the controller creates an access policy, default-mdns-policy which cannot be deleted. This is displayed with the Group Name and Description. Select the policy to view its Service Group details.

Click Save after editing the fields.

Configure a Controller's Application Visibility and Control (AVC) Parameters

Application Visibility and Control (AVC) uses the Network Based Application Recognition (NBAR) deep packet inspection technology to classify applications based on the protocol they use. Using AVC, the controller can detect more than 1400 Layer 4 to Layer 7 protocols. AVC enables you to perform real-time analysis and create policies to reduce network congestion, expensive network link usage, and infrastructure upgrades.

AVC is supported only on the Cisco 2500 and 5500 Series Controllers, and Cisco Flex 7500 and Cisco 8500 Series Controllers.

Set Up AVC Profiles on Controllers

To configure the AVC profile, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 Choose **Services** > **Application Visibility And Control** > **AVC Profile**from the left sidebar menu.

Step 4 Click the AVC Profile Name that you want to configure.

Step 5 To create AVC rules, click **Add.**

Step 6 Configure the following parameters:.

- Application Name—Name of the application.
- Application Group Name—Name of the application group to which the application belongs.
- Action—Drop-down list from which you can choose the following:
  - Drop—Drops the upstream and downstream packets corresponding to the chosen application.
  - Mark— Marks the upstream and downstream packets corresponding to the chosen application with the DSCP value that you specify in the Differentiated Services Code Point (DSCP) drop-down list. The DSCP value helps you provide differentiated services based on the QoS levels.

- Rate Limit—If you select Rate Limit as an action, you can specify Average Rate Limit per client and Burst data rate limit. The number of rate limit applications is limited to 3. The default action is to permit all applications.

- DSCP—Packet header code that is used to define quality of service across the Internet. The DSCP values are mapped to the following QoS levels:
  - Platinum (Voice)—Assures a high QoS for Voice over Wireless.
  - Gold (Video)—Supports the high-quality video applications.
  - Silver (Best Effort)—Supports the normal bandwidth for clients.
  - Bronze (Background)— Provides lowest bandwidth for guest services.
  - Custom—Specify the DSCP value. The range is from 0 to 63.
- DSCP Value—This value can be entered only when Custom is chosen from the DSCP drop-down list.
- Avg. Rate Limit (in Kbps)—If you select Rate Limit as an action, you can specify Average Rate Limit per client which is the average bandwidth limit of that application.
- Burst Rate Limit (in Kbps)—If you select Rate Limit as an action, you can specify Burst Rate limit which is the peak limit of that application.

Step 7 Click **Save**.

Related Topics

Configure a Controller's Multicast DNS (mDNS) Settings, on page 138
Configure a Controller's NetFlow Settings , on page 141
Configure a Device's Mesh Parameters , on page 120
Configure a Device's Port Parameters , on page 123
Configure a Controller's Management Parameters , on page 124
Configure a Controller's Location Information, on page 131
Configure a Controller's IPv6 Neighbor Binding and RA Parameters, on page 133
Configure a Controller's Proxy Mobile IPv6 (PMIP) Parameters, on page 135

Configure a Controller's NetFlow Settings

NetFlow is a protocol that provides valuable information about network users and applications, peak usage times, and traffic routing by collecting IP traffic information from network devices. The NetFlow architecture consists of the following components:

- Collector—An entity that collects all the IP traffic information from various network elements.
- Exporter—A network entity that exports the template with the IP traffic information. The controller acts as an exporter.

Configure NetFlow Monitor on the Controller

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 Choose **NetFlow** > **Monitor**from the left sidebar menu.

Step 4 Configure the following parameters:

- Monitor Name—Name of the NetFlow monitor. The monitor name can be up to 127 case-sensitive alphanumeric characters. You can configure only one monitor in the controller.
- Record Name—Name of the NetFlow record. A NetFlow record in the controller contains the following information about the traffic in a given flow:
  - Client MAC address
  - Client Source IP address
  - WLAN ID
  - Application ID
  - Incoming bytes of data
  - Outgoing bytes of data
  - Incoming Packets
  - Outgoing Packets
  - Incoming DSCP
  - Outgoing DSCP
  - Name of last AP

Step 5 Exporter Name—Name of the exporter. You can configure only one monitor in the controller.

Step 6 Exporter IP—IP address of the collector.

Step 7 Port Number—UDP port through which the NetFlow record is exported from the controller.

Step 8 Click **Save**.

Configure NetFlow Exporter on the Controller

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 Choose **NetFlow** > **Exporter** from the left sidebar menu.

Step 4 Configure the following parameters:

- Exporter Name—Name of the exporter.
- Exporter IP —IP address of the exporter.
- Port Number—The UDP port through which the Netflow record is exported.

Related Topics

Configure a Controller’s Multicast DNS (mDNS) Settings, on page 138
Configure a Controller’s NetFlow Settings , on page 141
Configure a Device's Mesh Parameters , on page 120
Configure a Device's Port Parameters , on page 123
Configure a Controller's Management Parameters , on page 124
Configure a Controller’s Location Information, on page 131
Configure a Controller’s IPv6 Neighbor Binding and RA Parameters, on page 133
Configure a Controller’s Proxy Mobile IPv6 (PMIP) Parameters, on page 135

Configure a Third-Party Controller or Access Point

Cisco Prime Infrastructure enables you to add third-party controllers and access points. As part of this feature you can perform the following functions:

- Add third-party controllers to the Cisco Prime Infrastructure.
- Monitor the state of the third-party controllers.
- Get inventory information for the third-party controllers and their associated access points.
- Use the background tasks to view the operations status third-party controllers and access points.

Related Topics

Add a Third-Party Controller, on page 143
View a Third-Party Controller's Operational Status, on page 144
View a Third-Party Access Point's Settings, on page 145
Remove a Third-Party Access Point, on page 145
View a Third-Party Controller's Operational Status, on page 144

Add a Third-Party Controller

To add a third-party controller, follow these steps:

Step 1 Choose Configuration > Network Devices > **Third Party** Wireless **Controller**.

Step 2 Click Add Device.

Step 3 In the Add Device page, enter the required parameters in the following tabs:

- General
- SNMP
- Telnet/SSH
- HTTP/HTTPS
- IPSec

Step 4 Click **Add**.

Related Topics

View a Third-Party Controller's Operational Status, on page 144
View a Third-Party Access Point's Settings, on page 145

Remove a Third-Party Access Point, on page 145
View a Third-Party Controller's Operational Status, on page 144

View a Third-Party Controller's Operational Status

To view the Third Party Controller Operational Status page, follow these steps:

Step 1 Choose **Administration** > **Settings** > **Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Third Party Controller Operational Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

- Enable the task.

  Select the **Third Party Controller Operational Status** check box. From the Select a command drop-down list, choose **Enable Tasks**, and click **Go**. The task converts from dimmed to available in the Enabled column.

- Disable the task.

  Select the **Third Party Controller Operational Status** check box. From the Select a command drop-down list, choose **Disable Tasks**, and click **Go**. The task is dimmed in the Enabled column after the disabling is complete.

Step 3 To modify the task, click the **Third Party Controller Operational Status** link in the Background Tasks column.

The Third Party Controller Operational Status page displays the Last Execution Information:

- Start Time.
- End Time.
- Elapsed Time (in seconds) of the task.
- Result—Success or error.
- Message—Text message regarding this task.

Step 4 View or modify the following in the Task Details section:

- Description—Display only. Displays the name of the task.
- Enabled—Select the check box to enable this task.
- Interval—Indicates the frequency (in minutes) of the task. The default is 3 hours.

Step 5 When finished, click **Save** to confirm task changes.

Related Topics

Add a Third-Party Controller, on page 143
View a Third-Party Access Point's Settings, on page 145
Remove a Third-Party Access Point, on page 145

View a Third-Party Access Point's Settings

The third-party access points are discovered when you add a third-party controller.

To view the configurations of a third-party access point, follow these steps:

Step 1 Choose **Configuration** > **Network Devices** > **Third Party Access Points**.

Step 2 Click the AP Name link to display the details. The General tab for that third-party access point appears.

Related Topics

Add a Third-Party Controller, on page 143
View a Third-Party Controller's Operational Status, on page 144
Remove a Third-Party Access Point, on page 145
View a Third-Party Controller's Operational Status, on page 144

Remove a Third-Party Access Point

To remove third-party access points, follow these steps:

Step 1 Choose **Configuration** > **Network Devices** > **Third Party Access Points**.

Step 2 Select the check boxes of the access points you want to remove.

Step 3 Click **Delete**.

Step 4 A confirmation message appears.

Step 5 Click **Yes**.

Related Topics

Add a Third-Party Controller, on page 143
View a Third-Party Controller's Operational Status, on page 144
View a Third-Party Access Point's Settings, on page 145
View a Third-Party Controller's Operational Status, on page 144

View a Third-Party Access Point's Operational Status

To view the Third Party Access Point Operational Status page, follow these steps:

Step 1 Choose **Administration** > **Settings** > **Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Third Party Access Point Operational Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

- Enable the task.

Select the **Third Party Access Point Operational Status** check box. From the Select a command drop-down list, choose **Enable Tasks**, and click **Go**. The task converts from dimmed to available in the Enabled column.

- Disable the task.

  Select the **Third Party Access Point Operational Status** check box. From the Select a command drop-down list, choose **Disable Tasks**, and click **Go**. The task is dimmed in the Enabled column after the disabling is complete.

Step 3 To modify the task, click the **Third Party Access Point Operational Status** link in the Background Tasks column.

The Third Party Controller Operational Status page displays the Last Execution Information:

- Start Time.
- End Time.
- Elapsed Time (in seconds) of the task.
- Result—Success or error.
- Message—Text message regarding this task.

Step 4 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select the check box to enable this task.
- Interval—Indicates the frequency (in minutes) of the task. The default is 3 hours.

Step 5 When finished, click **Save** to confirm task changes.

Related Topics

Add a Third-Party Controller, on page 143
View a Third-Party Controller's Operational Status, on page 144
View a Third-Party Access Point's Settings, on page 145
Remove a Third-Party Access Point, on page 145

View Switch Settings

Choose **Configuration** > **Network** > **Network Devices** > **Device Type** > **Switches and Hubs** to see a summary of all switches in the Cisco Prime Infrastructure database. Click any column heading to sort the information by that column. You can switch between ascending and descending sort order by clicking the column heading more than once.

Related Topics

View Switch Details, on page 146

View Switch Details

Choose **Configuration** > **Network** > **Network Devices** > **Device Type** > **Switches and Hubs**to see a summary of all switches in the Cisco Prime Infrastructure database. Click a Device Name to see detailed information about that switch.

Related Topics

Example: Configure SNMPv3 on Switches, on page 149

Change Switch SNMP Parameters

To modify SNMP parameters for a switch, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices** > **Device Type > Switches and Hubs**, then click the checkbox next to the switch for which you want to change SNMP credentials.

Step 2 Click **Edit**.

Step 3 Modify the necessary SNMP Parameters fields, then click one of the following:

- **Reset** to restore the previously saved parameters.
- **Save** to save and apply the changes you made.
- **Cancel** to exit without saving your changes and return to the previous screen.

Related Topics

View Switch Settings, on page 146
Example: Configure SNMPv3 on Switches, on page 149
Change Switch Telnet/SSH Credentials, on page 147

Change Switch Telnet/SSH Credentials

To modify Telnet or SSH parameters for a switch, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices** > **Device Type > Switches and Hubs**, then click the checkbox next to the switch for which you want to change Telnet or SSH credentials.

Step 2 Click **Edit**.

Step 3 Modify the necessary Telnet/SSH Parameters fields, then click one of the following:

- **Reset** to restore the previously saved parameters.
- **Save** to save and apply the changes you made.
- **Cancel** to exit without saving your changes and return to the previous screen.

Related Topics

View Switch Settings, on page 146
Example: Configure SNMPv3 on Switches, on page 149
Change Switch SNMP Parameters, on page 147

Add Switches

You can add switches to Prime Infrastructure database to view overall switch health and endpoint monitoring and to perform switchport tracing. The following switches can be configured:

- 3750
- 3560
- 3750E
- 3560E
- 2960.

The switch functionality appears on the configuration menu in Prime Infrastructure however you cannot configure switch features using Prime Infrastructure. You can only configure Prime Infrastructure system.

Prime Infrastructure allows you to do the following:

- Add switches in the **Configuration > Network > Network Devices** > **Device Type > Wireless Controller** page and specify CLI and SNMP credentials.
- Add a location-capable switch for tracking wired clients by mobility services engine and Prime Infrastructure in the **Configuration > Network > Network Devices** > **Device Type > Wireless Controller** page.
- Monitor Switches by choosing Monitor > Network Devices.
- Run switch-related reports using the Reports menu.

When you add a switch to the Prime Infrastructure database, by default, Prime Infrastructure verifies the SNMP credentials of the switch. If the device credentials are not correct, you receive an SNMP failure message but the switch is added to the Prime Infrastructure database.

Features Available by Switch Type

When you add a switch to Prime Infrastructure, you specify how the switch is to be managed, based on this, Prime Infrastructure determines the features that are available:

- Monitored switches—You can add switches (choose **Configuration > Network > Network Devices** > **Device Type > Wireless Controller**) and monitor switch operation (choose **Monitor > Network Devices**). Each switch counts as a single device against the total device count for your license. If you have unused device counts available in your license engine, you can add a switch to Prime Infrastructure. If you have no remaining device counts available, you cannot add additional switches to Prime Infrastructure.
- Switch Port Tracing (SPT) only switches—Switches perform switch port tracing only. SPT-only switches appear in the **Configuration > Network > Network Devices** > **Device Type > Switches and Hubs** page and in inventory reports. Licensing does not apply to SPT switches.

To add a switch to Prime Infrastructure, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices** > **Device Type > Switches and Hubs**, then click **Add Device**.

Step 2 Enter the appropriate information in the fields displayed.

See Cisco Pime Infrastrucutre Reference Guide, for more information.

Step 3 Click **Add** to add the switch or click **Cancel** to cancel the operation and return to the list of switches.

Related Topics

Import Switches From CSV Files, on page 149
Example: Configure SNMPv3 on Switches, on page 149

Example: Configure SNMPv3 on Switches

The following is an example for configuring SNMPv3 on the switch:

snmp-server view v3default iso includedsnmp-server group v3group v3 auth write v3default snmp-server user <username> <v3group> v3 auth <md5 or sha> <authentication password>

If the switch has VLANs, you must configure each VLAN, otherwise switch porting tracing fails. The following is an example if the switch has VLANs 1 and 20.

snmp-server group v3group v3 auth context vlan-1 write v3defaultsnmp-server group v3group v3 auth context vlan-20 write v3default

snmp-server group v3group v3 auth context vlan-20 write v3default

When you create SNMP v3 view, make sure you include all of the OIDs.

Related Topics

Import Switches From CSV Files, on page 149

Import Switches From CSV Files

You can import switches into the Cisco Prime Infrastructure database using a CSV file. The first row of the CSV file is used to describe the columns included. The IP Address column is mandatory.

The following example shows a sample CSV file.

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name, snmpv3_auth_type,
 snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries,
snmp_timeout,protocol,telnet_username,telnet_password,enable_password,telnet_timeout
16.1.1.3,255.255.255.0,v2,public,,,,,3,10,telnet,cisco,cisco,cisco,60
16.1.1.4,255.255.255.0,v2,public,,,,,3,10,ssh2,cisco,cisco,cisco,60
16.1.1.5,255.255.255.0,v2,public,,,,,3,10,,cisco,cisco,cisco,60
16.1.1.6,255.255.255.0,v2,public,,,,,3,10,telnet,cisco,cisco,cisco,60
3.3.3.3,255.255.255.0,v3,,default,HMAC-MD5,default,DES,default,3,4
4.4.4.4,255.255.255.0,v3,,default,HMAC-MD5,default,DES,default,3,4,telnet,cisco,cisco,cisco,60
```

The fields in the Civic Location pane are populated after the civic information is imported.

See Cisco Prime Infrastructure Reference Guide, for more information.

Related Topics

Add Switches, on page 148
Example: Configure SNMPv3 on Switches, on page 149

Remove Switches

When you remove a switch from the Prime Infrastructure database, the following functions are performed:

- Inventory information for that switch is removed from the database.
- Alarms for the switch remain in the database with a status of Clear. By default, cleared alarms are not displayed in the Prime Infrastructure interface.
- Saved reports remain in the database even if the switch on which the report was run is removed.

To remove a switch from Prime Infrastructure, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices** > **Device Type** > **Switches and Hubs**, then click the checkbox next to the switch for which you want to remove.

Step 2 Click **Delete**.

Step 3 Click **OK** to confirm the deletion.

Related Topics

Add Switches, on page 148

Example: Configure Switch Traps and Syslogs for Wired Clients

The following Cisco IOS configuration example shows how this Cisco IOS switch feature forwards SNMP traps from the switch to Prime Infrastructure server for MAC notifications (for on-802.1x clients):

```
snmp-server enable traps mac-notification change move threshold
snmp-server host<IP address of Prime Infrastructure server> version 2c <community-string>
mac-notification
mac address-table notification change interval 5
mac address-table notification change history-size 10
mac address-table notification change


interface <interface>
 description non-identity clients
 switchport access vlan <VLAN ID>
 switchport mode access
 snmp trap mac-notification change added  <- interface level config for MAC Notification
  snmp trap mac-notification change removed <- interface level config for MAC Notification
```

The debug command is:

```
debug snmp packets
```

The show command is:

```
show mac address-table notification change
```

See Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, for more information.

Example: Configure Syslog Forwarding for Catalyst Switches Using IOS

The syslog configuration forwards syslog messages from a Catalyst switch to the Prime Infrastructure server. This feature is used for identity clients discovery.The following Cisco IOS configuration example shows how this Cisco IOS switch forwards syslog messages from a Catalyst switch to the Prime Infrastructure server:

```
archive
 log config
  notify syslog contenttype plaintext
logging facility auth
logging <IP address of Prime Infrastructure server>
```

See Catalyst 3750 Software Configuration Guide, for more information.

Using Cisco OfficeExtend APs With Cisco Prime Infrastructure

An OfficeExtend access point provides secure communications from a controller to an access point at a remote location, seamlessly extending the corporate WLAN over the Internet to the residence of an employee. The experience of a teleworker at the home office is exactly the same as it is at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security.

Figure 25-1 **205774.jpg** illustrates a typical OfficeExtend access point setup.

OfficeExtend access points are designed to work behind a router or other gateway device that is using network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), thereby enabling an entire group of computers to be represented by a single IP address. In controller release 6.0, only one OfficeExtend access point can be deployed behind a single NAT device.

Currently, only Cisco Aironet 1130 series and 1140 series access points that are joined to a Cisco 5500 series controller with a WPlus license can be configured to operate as OfficeExtend access points.

Your firewall must be configured to allow traffic from access points using CAPWAP. Make sure that UDP ports 5246 and 5247 are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.

Before licensing for an OfficeExtend Access Point make sure that the WPlus license is installed on the 5500 series controller. After the license is installed, you can enable the OfficeExtend mode on an 1130 series or 1140 series access point.

The operating system software automatically detects and adds an access point to the Cisco Prime Infrastructure database as it associates with existing controllers in the Cisco Prime Infrastructure database.

Configure Link Latency to Measure the Link Between an AP and Controller

You can configure link latency on the controller to measure the link between an access point and the controller. This feature can be used with all access points joined to a controller but is especially useful for FlexConnect access points, for which the link could be a slow or unreliable WAN connection.

Link latency is supported for use only with FlexConnect access points in connected mode. FlexConnect access points in standalone mode are not supported.

Link latency monitors the round-trip time of the CAPWAP heartbeat packets (echo request and response) from the access point to the controller and back. This time can vary due to network link speed and controller processing loads. The access point timestamps the outgoing echo requests to the controller and the echo requests received from the controller. The access point sends this delta time to the controller as the system round-trip time. The access point sends heartbeat packets to the controller at a default interval of 30 seconds.

Link latency calculates the CAPWAP response time between the access point and the controller. It does not measure network latency or ping responses.

The controller displays the current round-trip time as well as a running minimum and maximum round-trip time. The minimum and maximum times continue to run as long as the controller is up or can be cleared and allowed to restart.

To configure link latency, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices** > **Device Type** > **Unified AP**, then click on a Device Name.

Step 2 Select the **Enable Link Latency** check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the controller after every echo response is received. The default value is unselected.

Step 3 Click **Save** to save your changes.

The link latency results appear below the Enable Link Latency check box:

a. Current—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.

b. Minimum—Because link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.

c. Maximum—Because the link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.

Step 4 To clear the current, minimum, and maximum link latency statistics on the controller for this access point, click **Reset Link Latency**. The updated statistics appear in the Minimum and Maximum fields.

Configure Unified APs

You can use the**Configuration** > **Network** > **Network Devices** > **Device Type** > **Unified AP** page to view and configure unified access points.

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then from the Device Groups menu on the left, select **Device Type** > **Wireless Controller**.

Step 2 Click an applicable IP address to view the following parameters:

- AP Name—Click an access point name to view or configure access point details.
- Base Radio MAC
- Admin Status
- AP Mode
- Software Version
- Primary Controller Name

Step 3 Click an access point name to view or configure the access point details. The displayed information might vary depending for the access point type.

Enable the Sniffer Feature on a Unified Access Point (AiroPeek)

When the sniffer feature is enabled on an access point, the access point functions as a sniffer and captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. The packets contain information on timestamp, signal strength, packet size, and so on.

The sniffer feature can be enabled only if you are running AiroPeek, which is a third-party network analyzer software that supports decoding of data packets. For more information on AiroPeek, see the following URL: www.wildpackets.com/products/airopeek/overview

Before You Begin

Before using the sniffer feature, you must complete the following:

- Configure an access point in sniffer mode at the remote site. For information on how to configure an access point in sniffer mode, see Configuring an AP in Sniffer Mode Using the Web User Interface in Related Topics.
- Install AiroPeek Version 2.05 or later on a Windows XP machine.
  - You must be a WildPackets Maintenance Member to download the following dll files. See the following URL: https://wpdn.wildpackets.com/view_submission.php?id=30
- Copy the following dll files:
  - socket.dll file to the Plugins folder (Example: C:\ProgramFiles\WildPackets\AiroPeek\Plugins)
  - socketres.dll file to the PluginRes folder (Example:C:\ProgramFiles\WildPackets\AiroPeek\1033\PluginRes)

Related Topics

Configure a Device's 802.11 Parameters , on page 113

Configure the AiroPeek Sniffer on a Remote Machine

To configure AiroPeek on the remote machine, follow these steps:

Step 1 Start the AiroPeek application and click **Options** on the Tools tab.

Step 2 Click **Analysis Module** in the Options page.

Step 3 Right-click inside the page and select **Disable All** option.

Step 4 Find the Cisco remote module column and enable it. Click **OK** to save the changes.

Step 5 Click **New capture** to bring up the capture option page.

Step 6 Choose the remote Cisco adapter and from the list of adapter modules.

Step 7 Expand it to locate the new remote adapter option. Double-click it to open a new page, enter a name in the text box provided and enter the controller management interface IP in the IP address column.

Step 8 Click **OK**. The new adapter is added to the remote Cisco adapter.

Step 9 Select the new adapter for remote airopeek capture using the access point.

Step 10 Click **start socket capture** in the capture page to start the remote capture process.

Step 11 From the controller CLI, bring up an access point, and set it to sniffer mode by entering the **config ap mode sniffer** *ap-name* command.

The access point reboots and comes up in sniffer mode.

Configure an AP in Sniffer Mode Using Cisco Prime Infrastructure

To configure an AP in Sniffer mode using the web user interface, follow these steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**, then click an item in the AP Name column to navigate to this page.

Step 2 In the General group box, set the AP mode to Sniffer using the drop-down list, and click **Apply**.

Step 3 Click a protocol (802.11a/802.11b/g) in the Protocol column in the Radio Interfaces group box. This opens the configuration page.

Step 4 Select the **Sniff** check box to bring up the Sniff parameters. Select the channel to be sniffed and enter the IP address of the server (The remote machine running AiroPeek).

Step 5 Click **Save** to save the changes.

Enable Flex+Bridge Mode on AP

To enable Flex+Bridge mode on your AP, follow these steps:

Step 1 Click **Configuration** > **Templates** > **Lightweight Access Points**.

Step 2 Click the relevant AP template or add a new template.

Step 3 Click **AP Parameters** tab and check the **AP Mode** checkbox.

Step 4 Select **Flex+Bridge** from the drop-down list and click **Save**.

- If you're switching the AP mode to or from Flex+Bridge, the AP goes for a reboot.
- Flex+Bridge mode does not support API encryption, AP Retransmit Interval, and only Critical AP Failover criteria is supported.
- Configurations made in FlexConnect and Mesh tabs does not provisioned when you change the AP mode. You first have to change the AP mode to Flex+Bridge and then configure parameters on FlexConnect and Mesh tabs.

Configure Controller Redundancy

"Controller Redundancy" refers to the High Availability (HA) framework embedded in controllers. Redundancy in wireless network controllers allows you to reduce network downtime. In a redundancy architecture, one controller is in the Active state and a second controller is in the Standby state. The Standby controller monitors the health of the Active controller continuously, using a redundant port. Both controllers share the same configurations including the IP address of the management interface.

The Standby or Active state of a controller is based on the redundancy stock keeping unit (SKU), which is a manufacturing-ordered unique device identifier (UDI). A controller with a redundancy SKU UDI is in the Standby state for the first time when it boots and pairs with a controller that runs a permanent count license. For controllers that have permanent count licenses, you can manually configure whether the controller is in the Active state or the Standby state.

Cisco Prime Infrastructure supports stateful switchover of access points (also known as "AP SSO"). AP SSO ensures that AP sessions remain intact despite controller switchovers. For more details on controller redundancy, see "Configuring Wireless Redundancy" in Related Topics.

Controller redundancy is similar to, but separate from, the Cisco Prime Infrastructure HA framework used to reduce Cisco Prime Infrastructure server downtime. For more information on this, see “Configuring High Availability” in Related Topics.

See Cisco Prime Infrastructire Administrator Guide, for more infromation.

Note Chassis Priority option will be disabled after WLC HA is established. The peer timeout and keep alive retires can be changed with HA mode configuration and to change any other configurations, HA should be disabled and reconfigured.

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats

Cisco Prime Infrastructure supports Cisco Adaptive Wireless Intrusion Prevention System (Cisco Adaptive wIPS, or wIPS), which uses profiles to quickly activate wireless threat protection features.

Cisco Prime Infrastructure provides a list of pre-defined wIPS profiles based on customer types, building types, and industry types, such as “Education”, “Financial”, “Military”, “Tradeshow”, and so on. You can use these profiles “as is” or customize them to better meet your needs. You can then apply them to the Mobility Services Engines and controllers you select.

Cisco Adaptive wIPS does not support the Cisco Prime Infrastructure partitioning feature.

See Cisco Wireless Intrusion Prevention System Configuration Guide for more information.

Related Topics

View wIPS Profiles, on page 155
Add wIPS Profiles, on page 156
Edit wIPS Profiles, on page 157
Apply wIPS Profiles, on page 158
Delete wIPS Profiles, on page 159

View wIPS Profiles

Prime Infrastructure wIPS Profiles List page provides access to wIPS profiles. You can use it to view, edit, apply or delete current wIPS profiles, and to create new wIPS profiles.

Choose **Services** > **Mobility Services** > **wIPS Profiles**. The wIPS Profiles List displays the list of current wIPS profiles. It gives the following information for each existing profile:

- Profile Name—The user-defined name for the wIPS profile.

  To view or edit a wIPS profile, click the Profile Name. Then follow the steps in “Edit wIPS Profiles” in Related Topics.

- Profile ID—The profile’s unique identifier.
- Version— The version of the profile.

- MSE(s) Applied To—Indicates the number of Mobility Services Engines (MSEs) to which this profile is applied. Click the MSE number to view profile assignment details.
- Controller(s) Applied To—Indicates the number of controllers to which this profile is applied. Click the controller number to view profile assignment details.

Related Topics

Add wIPS Profiles, on page 156
Edit wIPS Profiles, on page 157
Apply wIPS Profiles, on page 158
Delete wIPS Profiles, on page 159
Create SSID Groups, on page 159

Add wIPS Profiles

You can create new wIPS profiles using the default profile or any of the currently pre-configured profile.

Step 1 Select **Services > Mobility Services > wIPS Profiles**.

Step 2 Choose **Select a command > Add Profile > Go**.

Step 3 Type a profile name in the Profile Name text box of the Profile Parameters page.

Step 4 Select the applicable pre-defined profile, or choose **Default** from the drop-down list. Pre-defined profiles include the following:

- Education
- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen
- Hotspot8021x
- Military
- Retail
- Tradeshow
- Warehouse

Step 5 Click:

- **Save** to save the wIPS profile with no changes and no assignments. The profile appears in the profile list. You can access the profile for edits and assignment later, as explained in “Accessing wIPS Profiles” in Related Topics.

- **Save and Edit** to save the profile, edit its settings, and assign it to Mobility Services Engines and Controllers. For details, see “Editing wIPS Profiles” in Related Topics.

Related Topics

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats , on page 155
View wIPS Profiles, on page 155
Edit wIPS Profiles, on page 157

Edit wIPS Profiles

The wIPS profile editor allows you to configure profile details, including the following:

- SSID groups—Select the SSID groups to which the wIPS profile will be applied.
- Policy inclusion—Determine which policies are included in the profile.
- Policy level settings—Configure settings for each policy included in the profile, such as threshold, severity, notification type, and ACL/SSID groups.
- MSE/controller applications—Select the MSEs and controllers to which you want to apply the profile.

Step 1 Access the wIPS profile editor by:

- Create a new wIPS profile and then click **Save and Edit**.
- Choose **Services** > **Mobility Services** > **wIPS Profiles**and then click the Profile Name of the wIPS profile you want to edit.

  Prime Infrastructure displays the SSID Group List page. Using this page, you can edit and delete current SSID groups or add a new group. You can also select from the global list of SSID groups. For details, see “Associating SSID Groups With wIPS Profiles” in Related Topics.

Step 2 Select the SSID groups you want to associate with the wIPS profile, then click **Save**.

Step 3 Click Next. The Profile Configuration page displays.

Step 4 In the Select Policy pane’s policy tree, select the check boxes of the policies you want to enable or disable in the current profile.

You can enable or disable an entire branch or an individual policy by selecting the check box for the applicable branch or policy.

By default, all policies are selected.

Step 5 In the Profile Configuration page, click an individual policy to display the policy description and to view or modify current policy rule settings. The following options are available for each policy:

- Add—Click **Add** to access the Policy Rule Configuration page to create a new rule for this policy.
- Edit—Select the check box of the applicable rule, and click **Edit** to access the Policy Rule Configuration page to edit the settings for this rule.
- Delete—Select the check box of the rule you want to delete, and click **Delete**. Click **OK** to confirm the deletion.

  There must be at least one policy rule in place. You cannot delete a policy rule if it is the only one in the list.
- Move Up—Select the check box of the rule you want to move up in the list. Click **Move Up**.

- Move Down—Select the check box of the rule you want to move down in the list. Click **Move Down**.

  The following settings can be configured at the policy level:

- Threshold (not applicable to all policies)—Indicates the threshold or upper limit associated with the selected policy. When the threshold is reached for a policy, an alarm is triggered.

  Because every policy must contain at least one threshold, default thresholds are defined for each based on standard wireless network issues.

  Threshold options vary based on the selected policy.

  Alarms from Cisco Adaptive wIPS DoS and security penetration attacks are classified as security alarms. A summary of these attacks is located in the Security Summary page. Choose **Monitor > Security** to access this page. The wIPS attacks are located in the Threats and Attacks section.

- Severity—Indicates the level of severity of the selected policy. Parameters include critical, major, info, and warning. The value of this field might vary depending on the wireless network.

- Notification—Indicates the type of notification associated with the threshold.

- ACL/SSID Group—Indicates the ACL or SSID Group(s) to which this threshold is be applied.

  Only selected groups trigger the policy.

Step 6 When the profile configuration is complete, click **Save** to save your changes to the profile.

Step 7 Click **Next** to display the MSE/Controller(s) page.

Step 8 In the Apply Profile page, select the check boxes of the MSEs and controllers to which you want to apply the current profile.

Step 9 When you are finished, click **Apply** to apply the current profile to the selected MSEs and controllers.

You can also apply a newly created profile directly from the Profile List page. See “Applying wIPS Profiles” in Related Topics.

Related Topics

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats , on page 155
View wIPS Profiles, on page 155
Apply wIPS Profiles, on page 158
Delete wIPS Profiles, on page 159
Create SSID Groups, on page 159

Apply wIPS Profiles

Step 1 Choose **Services > Mobility Services > wIPS Profiles**.

Step 2 Select the check boxes of the wIPS profiles you want to apply.

Step 3 Choose **Select a command > Apply Profile > Go**.

Step 4 Select the mobility services engines and controllers to which you want the profile applied.

If the new profile assignment is different from the current assignment, you are prompted to save the profile with a different name.

Step 5 Click **Apply.**

Related Topics

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats , on page 155
Create SSID Groups, on page 159

Delete wIPS Profiles

Profiles currently applied to MSEs and controllers cannot be deleted.

Step 1 Choose **Services** > **Mobility Services** > **wIPS Profiles**.
Step 2 Select the check boxes of the wIPS profiles you want to delete.
Step 3 Choose **Select a command** > **Delete Profile** > **Go**.
Step 4 Click **OK** to confirm the deletion.

Related Topics

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats , on page 155
Add wIPS Profiles, on page 156
Edit wIPS Profiles, on page 157
Apply wIPS Profiles, on page 158

Associate SSID Groups With wIPS Profiles

The SSID (Service Set IDentifier) is a token or key which identifies an 802.11 (Wi-Fi) network. Users must either know or be able to discover the SSID to join an 802.11 network.

You can associate SSIDs with a wIPS profile by adding the SSIDs to an SSID group, then associating the SSID group with the wIPS profile.

Related Topics

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats , on page 155
Delete wIPS Profiles, on page 159
Create SSID Groups, on page 159
Edit SSID Groups, on page 160

Create SSID Groups

Step 1 Choose **Services** > **Mobility Services** > **wIPS Profiles**.
Step 2 Click the Profile Name of any wIPS profile. Prime Infrastructure displays the SSID Group List page.
Step 3 Choose **Select a command** > **Add Group** > **Go**.
Step 4 Enter the SSID Group Name in the text box.
Step 5 Enter the SSIDs in the SSID List text box. Enter multiple SSIDs with a carriage return after each SSID.
Step 6 Click **Save**.

Related Topics

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats , on page 155
Associate SSID Groups With wIPS Profiles, on page 159

Edit SSID Groups

Step 1 Choose **Services** > **Mobility Services** > **wIPS Profiles**.
Step 2 Click the Profile Name of any wIPS profile. Prime Infrastructure displays the SSID Group List page.
Step 3 Select the check box of the SSID group that you want to edit.
Step 4 Choose **Select a command** > **Edit Group** > **Go**.
Step 5 Make the necessary changes to the SSID Group Name or the SSID List.
Step 6 Click **Save**.

Related Topics

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats , on page 155
View wIPS Profiles, on page 155

Delete SSID Groups

Step 1 Choose **Services** > **Mobility Services** > **wIPS Profiles**.
Step 2 Click the Profile Name of any wIPS profile. Prime Infrastructure displays the SSID Group List page.
Step 3 Select the check boxes of the SSID groups that you want to delete.
Step 4 Choose **Select a command** > **Delete Group** > **Go**.
Step 5 Click **OK** to confirm the deletion.

Related Topics

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats , on page 155
View wIPS Profiles, on page 155
Edit wIPS Profiles, on page 157

Configure High Availability for MSE Servers

You can use Cisco Prime Infrastructure to pair and manage Cisco Mobility Services Engine (MSE) devices that have been configured for MSE High Availability (HA). The following related topics explain how to perform these and related tasks.

Related Topics

MSE HA Server Failover and Failback, on page 161
Configure the MSE HA Servers, on page 161
View Details About the Primary and Secondary MSE HA Server, on page 162
View MSE Server HA Status, on page 163
Trigger MSE HA Manual Failover or Failback, on page 163

Configure Automatic HA Failover and Failback on MSE Servers, on page 164

MSE HA Server Failover and Failback

The MSE HA feature is intended to permits continued access to MSE services even when the primary MSE fails. The secondary MSE maintains a complete copy of the primary MSE's data, serving as its backup. Health Monitor and "heartbeat" processes running on both the primary and secondary keep each server informed about the state of the other.

Whenever the primary MSE fails, a "failover" to the secondary MSE is triggered. Prime Infrastructure will then use the secondary's mobility services instead of the primary until the problems with the primary are fixed.

When the primary is back in service, a "failback" is triggered, returning control to the primary MSE, and replicating data about the intervening state of the network back to the primary from the secondary MSE.

When configuring MSE HA, you can choose to have failovers triggered either automatically or manually. You have the same options for failbacks.

Configuring MSE HA for manual failover or failback means these operations must be triggered by a user, in response to critical alarms sent when the primary fails or is restored to service.

Configuring MSE HA for automatic failover reduces the need for network administrators to manage MSE HA. It also reduces the time taken to respond to the conditions that provoked the failover, since it brings up the secondary server automatically, within approximately 10 seconds (the default) of detection of failure on the primary. If MSE HA is configured for automatic failback, the system will trigger the failback only after successful receipt of 30 ping messages sent once per minute.

Related Topics

Configure the MSE HA Servers, on page 161
Configure Automatic HA Failover and Failback on MSE Servers, on page 164
Configure High Availability for MSE Servers, on page 160

Configure the MSE HA Servers

In order to activate High Availability for MSE devices, you must create a pairing, where one MSE serves as the primary MSE device, and another acts as the secondary MSE.

Note that you can only pair MSE devices that are:

- Properly configured for use with MSE High Availability, as explained in the related topic "Configuring MSE High Availability".
- Added to Prime Infrastructure, as explained in the related topic "Adding MSEs to Prime Infrastructure".

Before You Begin

To create the pairing, you will need to know:

- The device name of the primary MSE server.
- The device name of the secondary MSE server. This can be a previously assigned device name, or a new name you assign at the moment you pair the servers.
- The secondary MSE HA server's IP address. This is the IP address of the HA Health Monitor, which was assigned when configuring the MSE server for HA use.
- The secondary MSE HA server's password. This is the Prime Infrastructure communication password, which was assigned when configuring the MSE server for HA use.

You must also decide if you want to configure the MSE HA servers for manual or automatic failback. For guidelines, see the related topic "MSE HA Automatic vs Manual Failover and Failback".

Step 1 Choose **Services** > **Mobility Services** > **Mobility Services Engines**. A list of the existing MSEs is displayed.

Step 2 In the list, find the MSE you want to act as the primary MSE HA server.

Step 3 The "Secondary Server" column for the MSE listing displays the message "N/A (Click here to configure)". Click on the link to display the HA configuration page for the primary MSE.

Step 4 Enter the secondary MSE's device name, Health Monitor IP address, and Prime Infrastructure communication password in the appropriate fields.

Step 5 Specify the failover and failback types. You can choose either Manual or Automatic

Step 6 Specify the Long Failover Wait. This is the maximum time the system will wait to trigger automatic failover after detection of primary MSE failure. The default is 10 seconds; the maximum is 120 seconds.

Step 7 Click **Save**. Prime Infrastructure prompts you to confirm that you want to pair these MSEs. Click **OK** to confirm.

Prime Infrastructure conducts the pairing and synchronization automatically. These processes can take up to 20 minutes to complete, depending on network bandwidth and many other factors. To check on the progress of these processes, select **Services** > **Mobility Services Engine** > **System** > **Services High Availability** > **HA Status**.

Related Topics

MSE HA Server Failover and Failback, on page 161
Configure Automatic HA Failover and Failback on MSE Servers, on page 164
Configure High Availability for MSE Servers, on page 160

View Details About the Primary and Secondary MSE HA Server

Step 1 Choose **Services** > **Mobility Services** > **Mobility Services Engines**.

Step 2 To see the HA parameters for the:

- Primary MSE HA server: Click the name of the server in the **Device Name** column.
- Secondary MSE HA server: Click the name of the server in the **Secondary Server** column.

Prime Infrastructure displays the Mobility Services Engines configuration page for the server you selected.

Step 3 In the left sidebar menu, choose HA Configuration. The HA Configuration page provides the following information:

- Primary Health Monitor IP
- Secondary Device Name
- Secondary IP Address
- Secondary Password
- Secondary Platform UDI
- Secondary Activation Status
- Failover Type

- Failback Type
- Long Failover Wait

Related Topics

Configure the MSE HA Servers, on page 161
Trigger MSE HA Manual Failover or Failback, on page 163
View MSE Server HA Status, on page 163
Configure Automatic HA Failover and Failback on MSE Servers, on page 164
Configure High Availability for MSE Servers, on page 160

View MSE Server HA Status

Step 1 Choose **Services** > **Mobility Services** > **Mobility Services Engines**.

Step 2 To see the HA status of the:

- Primary MSE HA server: Click the name of the server in the **Device Name** column.
- Secondary MSE HA server: Click the name of the server in the **Secondary Server** column.

Prime Infrastructure displays the Mobility Services Engines configuration page for the server you selected.

Step 3 In the left sidebar menu, choose HA Status. The Current High Availability Status page shows the following information:

- Status—Shows whether the MSE HA server is active and correctly synchronized.
- Heartbeats—Shows whether the MSE HA server is exchanging heartbeat signals with its partner.
- Data Replication—Shows whether MSE HA server is replicating data with its partner.
- Mean Heartbeat Response Time—Shows the mean heartbeat response time between servers.
- Events Log—Shows the last 20 events that the MSE server has generated.

Step 4 Click **Refresh Status** to update the MSA server's HA status information and Events Log.

Related Topics

Configure the MSE HA Servers, on page 161
View Details About the Primary and Secondary MSE HA Server, on page 162
Configure Automatic HA Failover and Failback on MSE Servers, on page 164
Configure High Availability for MSE Servers, on page 160

Trigger MSE HA Manual Failover or Failback

Manual failover and failback are enabled by default. Manual configuration requires that the Prime Infrastructure administrator trigger failovers and failbacks manually, in response to system alarms.

You can also configure paired MSE HA servers for automatic failover and failback (see Related Topics).

Step 1 Choose **Services** > **Mobility Services** > **Mobility Services Engines**.

Step 2 To trigger a:

- Failover from the primary to the secondary: Click the name of the primary MSE HA server in the **Device Name** column.
- Failback from the secondary to the primary: Click the name of the secondary MSE HA server in the **Secondary Server** column.

Prime Infrastructure displays the Mobility Services Engines configuration page for the server you selected.

Step 3 In the left sidebar menu, choose HA Configuration. The HA Configuration page displays the HA configuration information for the server you chose.

Step 4 Click **Switchover** to initiate the failover or failback.

Step 5 Click **OK** to confirm that you want to initiate the switchover.

Related Topics

MSE HA Server Failover and Failback, on page 161
Configure Automatic HA Failover and Failback on MSE Servers, on page 164
Configure High Availability for MSE Servers, on page 160

Configure Automatic HA Failover and Failback on MSE Servers

Manual failover and failback are enabled by default. If you configure paired MSE HA servers for automatic failover and failback, the change will occur automatically, as follows:

- Failover from primary to secondary: Triggered immediately, as soon as the secondary detects a failure on the primary.
- Failback from secondary to primary: Triggered after 30 successful ping messages from the secondary to the primary. Ping requests are sent once per minute.

Step 1 Choose **Services** > **Mobility Services** > **MSE High Availability**.

Step 2 Click the name of the primary MSE HA server in the **Device Name** column.

Prime Infrastructure displays the HA Configuration page for the primary MSE HA server.

Step 3 In the **Failover Type** and **Failback Type** list boxes, select **Automatic**.

Step 4 If needed: Change the value in **Long Failover Wait** to control the maximum delay between detection of a failure on the primary and automatic failover. The default is 10 seconds.

Step 5 Click **Save** to save your changes.

Related Topics

MSE HA Server Failover and Failback, on page 161
Trigger MSE HA Manual Failover or Failback, on page 163
Configure High Availability for MSE Servers, on page 160

Unpair MSE HA Servers

Step 1 Choose **Services** > **Mobility Services** > **MSE High Availability**.

Step 2 Click the name of the primary MSE HA server in the **Device Name** column.

Prime Infrastructure displays the HA Configuration page for the Primary MSE HA server.

Step 3 Click **Delete** to unpair the MSE servers.

Step 4 Click **OK** to confirm that you want to unpair the MSE HA servers.

Related Topics

Configure the MSE HA Servers, on page 161
Configure High Availability for MSE Servers, on page 160

Configure Controllers Using Plug and Play

Auto provisioning allows Cisco Prime Infrastructure to automatically configure a new or replace a current wireless LAN controller (WLC). Cisco Prime Infrastructure auto provisioning feature can simplify deployments for customers with a large number of controllers.

For Auto Provisioning privileges, you must have Admin, Root, or SuperUser status.

To allow or disallow a user Auto Provisioning privileges, edit the permitted tasks using Administration Settings > Users, Roles, and AAA > User Groups > *group name* > List of Tasks Permitted in Cisco Prime Infrastructure. Select or unselect the check box to allow or disallow these privileges.

A controller radio and b/g networks are initially disabled by the Cisco Prime Infrastructure downloaded startup configuration file. If desired, you might turn on those radio networks by using a template, which should be included as one of the automated templates.

To specify the Auto Provision filter contents, you can directly enter the details in the application or import the details from a CSV file. The auto provisioning feature supports the 5500 and non-5500 series controllers. The non-5500 series controllers have AP manager interface configuration information defined, whereas 5500 series controllers do not have this information.

To access the Auto Provisioning feature, choose **Configuration** > **Plug and Play** > **WLC Auto Provisioning**.