Monitor Tab

The Monitor tab on the menu bar enables you to access the controller and APs' summary details. Use the left navigation pane to access the respective network details.

Information available via the Monitor tab:

- Summary
- Access Points
- Cisco CleanAir
- Statistics
- Cisco Discovery Protocol
- Rogues
- Redundancy
- Clients
- Sleeping Clients
- Multicast Groups
- Applications
- Lync
- Local Profiling

Summary

Choose **MONITOR > Summary** to navigate to the Summary page.

The summary page provides a top level description of your controller, access points, clients, WLANs, and rogues. Rogues are unauthorized devices (access points, clients) that are connected to your network.

The controller image is displayed at the top of the summary page and gives information about the controller model number and the number of access points supported by the controller.

Note All parameters on this page are read-only parameters.

This page is automatically refreshed every 30 seconds.

This table describes the monitor summary parameters.

Table 2-1 Summary Parameters

Parameters	Description
Controller Summary	
Management IP Address	Management IPv4/IPv6 address of the controller. From Release 8.0, IPv6 is also supported for configuring Management interface.
Service Port IP Address	IPv4/IPv6 address of the controller front-panel service port. From Release 8.0, IPv6 is also supported for configuring Service interface.
Software Version	Version of the Operating System running on the controller.
Field Recovery Image Version	Version of the boot software ER.aes file. **Note** If a boot software ER.aes file is not installed, the Field Recovery Image Version field shows an error.
System Name	Controller name specified by the operator.
Up Time	Time elapsed since the controller was last rebooted.
System Time	Current time set on the controller.
Redundancy Mode	Redundancy mode operational on the device. The redundancy modes are as follows: • 0—No redundancy • SSO—Hot Standby Mode • RPR—Cold Standby Mode
Internal Temperature	The internal temperature of the controller.
802.11a/n Network State	Network that is enabled or disabled.
802.11b/g/n Network State	Network that is enabled or disabled.
Local Mobility Group	Name of the default mobility group.
CPU Usage	Percentage of the CPU in use.
Individual CPU Usage (5500 series controller only)	Percentage of the CPU in use and the percentage of the CPU time spent at the interrupt level. This field appears only for the Cisco 5500 Series Controller.
Memory Usage	Percentage of memory in use.
Access Point Summary	
802.11a/n/ac Radios	Number of 802.11a/n Cisco Radios. Click **Detail** for additional information about 802.11a/n/ac Radios.
802.11b/g/n Radios	Number of 802.11b/g/n Cisco Radios. Click **Detail** for additional information about 802.11b/g/n Radios.
Dual-Band Radios	Number of 802.11a/b/g/n Cisco Radios. Click **Detail** for additional information about Dual-Band Radios.
All APs	Number of access points associated with this controller. Click **Detail** for additional information about All APs.
Client Summary	
Current Clients	Number of clients currently associated with the controller. Click **Detail** for additional information about current Clients.

Table 2-1 Summary Parameters

Parameters	Description
Excluded Clients	Number of excluded client computers by MAC address that you can enable or disable. Click **Detail** for additional information about excluded clients.
Disabled Clients	Number of clients that are currently disabled. Click **Detail** for additional information about disabled clients.
Rogue Summary	
Active Rogue APs	Number of unauthorized access points detected by the controller. Click **Detail** for additional information about active Unclassified Rogue APs.
Active Rogue Clients	Number of active clients associated with a rogue access point. Click **Detail** for additional information about Rogue Client Details.
Adhoc Rogues	Number of ad-hoc rogues. Click **Detail** for additional information about Adhoc Rogues.
Rogues on Wired Network	Number of rogues on a wired network. Click **Detail** for additional information.
Session Timeout	
Session Timeout	• If you leave the check box unchecked, the **Monitor > Summary** page gets refreshed every 30 seconds. • If you check the check box, the **Monitor > Summary** page does not get refreshed automatically every 30 seconds.
Top WLANs	
Profile Name	Name of the WLAN as specified by the operator.
# of Clients by SSID	Number of clients associated with the WLAN based on SSID.
Most Recent Traps	Log of most recent SNMP traps. Click **View All** to view all SNMP Trap Logs.
Top Applications	
Application Name	Top 10 applications detected by the Cisco WLC in the last three minutes that appear according to their total byte count. These applications include both upstream and downstream applications.
Packet Count	Packet count of the application.
Byte Count	Byte count of the application.
Top Flex Applications	
Application Name	Top 10 FlexConnect applications detected by the Cisco WLC in the last three minutes that appear according to their total byte count. These applications include both upstream and downstream applications.
Packet Count	Packet count of the application.
Byte Count	Byte count of the application.

Access Points

Choose **MONITOR > Access Points** to navigate to the Access Points page. From here you can choose the following:

- **MONITOR > Access Points > Radios > 802.11a/n/ac** to view the Cisco radio profile for your 802.11a/n/ac RF network.
- **MONITOR > Access Points > Radios > 802.11b/g/n** to view the Cisco radio profile for your 802.11b/g/n RF network.
- **MONITOR > Access Points > Radios > Dual-Band Radios** to view the Cisco radio profile for your 802.11a/b/g/n RF network.

802.11a/n/ac Radios

Choose **MONITOR > Access Points > Radios** > **802.11a/n/ac** to navigate to the 802.11a/n/ac Radios page.

The 802.11a/n/ac Radios page displays the Cisco Radio profile for your 802.11a/n/ac RF network. The page also displays the status of each 802.11a/n/ac Cisco Radio that is configured on the controller and its profile.

AP List Filter

Click **Change Filter** to display the Search APs dialog box (see the figure below) and to create or change filter parameters. Click **Clear Filter** to remove the filter and display the entire access point list.

You can create a filter to display the list of access points by MAC address or AP name.

The following filter parameters are displayed in the Current Filter field.

- MAC Address—MAC address.
- AP Name—Access point name.
- CleanAir Oper Status—Operational status of the CleanAir-capable access point. Choose from the following available statuses:
  - UP
  - DOWN
  - ERROR
  - N/A

Note When you enable filtering by the MAC address, the other filters are disabled automatically. However, you can use a combination of the AP Name and CleanAir Oper Status to filter access points.

Click **Find** to commit your changes. Only the access points that match your search criteria appear on the 802.11a/n/ac Radios page. The Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

Note If you want to remove the filter and display the entire access point list, click **Clear Filter**.

802.11a/n/ac and 802.11b/g/n Radio Profile

To access the details for each Cisco Radio, click the **Detail** link (see Radio Statistics for more information).

To access the details of air quality, click the blue arrow adjacent the desired radio and click **CleanAir** (see Cisco CleanAir for more information).

This table describes the 802.11a/n /ac radio parameters.

Table 2-2 802.11a/n /ac Radio Parameters

Parameters	Description
AP Name	Name assigned to the access point.
Radio Slot #	Slot where the radio is installed.
Base Radio MAC	MAC address of the access point.
Sub Band	Radio sub band, if it is active: 4.9 GHz or 5.8 GHz.
Operational Status	Operational status of the Cisco Radios: UP or DOWN.
Radio Role	Radio role: UPLINK or DOWNLINK.
Load Profile	Radio Resource Management (RRM) profile for the Cisco Radio. The profile status is displayed as a pass or fail with details provided on the Radio Statistics page. **Note** For Cisco OEAP 600 Series access points, the following parameters show the value as N/A: – Load Profile – Noise Profile – Interference Profile – Coverage Profile
Noise Profile	
Interference Profile	
Coverage Profile	
CleanAir Admin Status	CleanAir admin status.
CleanAir Oper Status	Spectrum sensor status for this access point.

Radio Statistics

Choose **MONITOR > Access Points > Radios > 802.11a/n/ac** or **802.11b/g/n**, click the blue arrow adjacent the desired access point and choose **Detail** to navigate to the Radio Statistics page.

Note Rx Neighbors, Radar Information, and Band Select Statistics are not displayed for outdoor mesh access points.

This page displays the RF (Radio Frequency) statistics for the selected Cisco Radio. You can alternate between the Graphics View and the Text View by clicking the **Graphics View/Text View** button. You can view and refresh detailed statistics by selecting them (using the check boxes) and then clicking the **Refresh** button on the data page.

Link Parameters

These parameters are displayed for 802.11a/n/ac radios on Mesh access points.

- Radio Role—Radio role for the backhaul: UPLINK or DOWNLINK.
- Source Backhaul MAC—MAC address of the source backhaul radio.

VoIP Stats

Note VoIP Stats parameters are not displayed for outdoor mesh access points.

The VoIP Stats shows the cumulative number and length of voice calls for this access point radio. Entries are added automatically when voice calls are successfully placed and deleted when the access point disassociates from the Cisco WLC.

SIP CAC Call Stats

Note The SIP CAC Call Stats parameters are not displayed for outdoor mesh access points.

The SIP CAC Call stats section shows the following information:

- Total number of SIP calls in progress
- Number of roaming SIP calls in progress
- Total number of SIP calls since AP joined
- Total number of roaming SIP calls since AP joined
- Total number of SIP calls rejected due to insufficient bandwidth
- Total number of SIP roam calls rejected due to insufficient bandwidth
- Total number of SIP calls rejected due to maximum call limit
- Total number of SIP roam calls rejected due to maximum call limit

Preferred Call Stats

The Preferred Call Stats section shows the following information:

- Total number of preferred calls received
- Total number of preferred calls accepted

KTS CAC Call Stats

The KTS CAC Call Stats section shows the following information:

- Total number of KTS calls in progress
- Number of roaming KTS calls in progress
- Total number of KTS calls since AP joined
- Total number of roaming KTS calls since AP joined
- Total number of KTS calls rejected due to insufficient bandwidth
- Total number of KTS roam calls rejected due to insufficient bandwidth

Video Call Admission Control (CAC) Stats

The Video Call Admission Control (CAC) Stats section shows the following information:

- Video Bandwidth in use (% of config bandwidth)
- Video Roam Bandwidth in use (% of config bandwidth)
- Total Bandwidth in use for Video

TPSEC Video CAC Call Stats

The TPSEC Video CAC Call Stats section shows the following information:

- Total number of video calls in progress
- Number of roaming video calls in progress
- Total number of video calls since AP joined
- Total number of roaming video calls since AP joined
- Number of video calls rejected since AP joined
- Number of roaming video calls rejected since AP joined
- Number of video calls rejected due to insufficient bandwidth
- Number of video roam calls rejected due to invalid parameters
- Number of video roam calls rejected due to the physical layer (PHY) rate
- Number of video roam calls rejected due to the QoS policy

SIP Video CAC Call Stats

The SIP Video CAC Call Stats section shows the following information:

- Total number of video calls in progress
- Number of roaming video calls in progress
- Total number of video calls since AP joined
- Total number of roaming video calls since AP joined
- Number of video calls rejected due to insufficient bandwidth
- Number of roaming video calls rejected due to insufficient bandwidth

Profile Information—Graphics View and Text View

The RF statistics are used to derive the RRM profile for each Cisco Radio in your network (see the following figure). The controller uses the Radio Resource Management (RRM) profile to adjust the Cisco Radio transmit and receive levels in order to maintain the most efficient configuration for your network. This data view also displays the RF properties of the controller and its clients.

- The Radio Resource Management (RRM) PASSED/FAILED thresholds are globally set for all access points in the 802.11a/n/ac RF Grouping and 802.11b/g/n RF Grouping pages.
- The Radio Resource Management (RRM) PASSED/FAILED thresholds are individually set for this access point in the Performance Profile of 802.11a/n/ac Access Points page.

Click **Graphics View** to view the RRM profile information as a graph.

Click **Text View** to view the RRM profile information as tables.

The following sections describe each of the Graphical and Text results.

Noise vs. Channel

Each channel of the access point appears with the corresponding non-802.11 noise that interferes with the currently assigned channel.

Interference by Channel

Each channel of the access point appears with the corresponding traffic interference from other 802.11 sources.

Load Statistics

The total Receive and Transmit bandwidth and channel utilization appears for transmitting and receiving traffic on this Cisco Radio. The number of attached clients is also displayed.

% Client Count vs. RSSI

This graphic view sorts attached clients by their Received Signal Strengths.

% Client Count vs. SNR

This graphic view sorts attached clients by their Signal to Noise Ratios.

Rx Neighbors Information

This area displays the Cisco Radio's neighboring access points and their IP address and RSSI values. These details are used for channel allotment and RF coverage area shaping.

Information similar to the following appears:

```
AP 00:0b:85:00:83:00 Interface 0         172.16.16.10
```

where

- AP is an access point.
- 00:0b:85:00:83:00 is the MAC address of the neighboring access point.
- Interface x is the interface number of the neighboring access point.
- 172.16.16.10 is the IP address of the access point's controller.

Radar Information

The Dynamic Frequency Selection (DFS) capability of the Cisco IOS software detects radar signals (typically military and weather) within the operating range of the access point. If a radar is detected, then the Cisco IOS access point will decide which channel to go on and report that information to the Cisco WLC. The Cisco WLC will then be responsible for maintaining a 30-minute timeout for the channels on which the radar was detected. When the access point is in FlexConnect standalone mode, it changes the channel when it detects a radar and reports back to the Cisco WLC after the next successful join.

802.11 MAC Counters

Table 2-3 802.11 MAC Counters

Counter	Description
Tx Fragment Count	Counter that is incremented for an acknowledged MPDU (MAC Protocol Data Unit) with an individual address in the address 1 field.
Tx Failed Count	Counter that increments when an MSDU (MAC Service Data Unit) is successfully transmitted after one or more retransmissions.
Multiple Retry Count (Graphics view only)	Counter that increments when an MSDU is successfully transmitted after more than one retransmission.
RTS Success Count	Counter that increments when a CTS (Clear To Send) is received in response to an RTS (Request To Send).
ACK Failure Count	Counter that increments when an ACK is not received when expected.
Multicast Rx Frame Count	Counter that increments when an MSDU is received with the multicast bit set in the destination MAC address.
Tx Frame Count	Counter that increments for each successfully transmitted MSDU.
Multicast Tx Frame Count	Counter that increments only when the multicast bit is set in the destination MAC address of a successfully transmitted MSDU. When operating as a STA in an ESS, where these frames are directed to the access point, this frame count implies having received an acknowledgment to all associated MPDUs.
Retry Count	Counter that increments when an MSDU is successfully transmitted after one or more retransmissions.
Frame Duplicate Count	Counter that increments when a frame is received that the Sequence Control field indicates is a duplicate.
RTS Failure Count	Counter that increments when a CTS is not received in response to an RTS.
Rx Fragment Count	Counter that increments for each successfully received MPDU of type Data or Management.
FCS Error Count	Counter that increments when an FCS error is detected in a received MPDU.
WEP Undecryptable Count	Counter that increments when a frame received with the WEP subfield of the Frame Control field is set to one and the WEP On value for the key that is mapped to the MAC address of the TA indicates that the frame should not have been encrypted or that the frame has been discarded because to the receiving STA has not implemented the privacy option.

Band Select Statistics

The Band Select Statistics section shows the following information:

- Number of dual band client
- Number of dual band client added
- Number of dual band client expired
- Number of dual band client replaced

- Number of dual band client detected
- Number of suppressed client
- Number of suppressed client expired
- Number of suppressed client replaced

CleanAir Parameters

The CleanAir operational status is displayed by the **Operational Status** parameter.

802.11b/g/n Radios

Choose **MONITOR > Access Points > Radios > 802.11b/g/n** to navigate to this page.

This page displays the Cisco Radio profile for your 802.11b/802.11g RF network. It shows the status of each 802.11b/g Cisco Radio configured and its profile.

AP List Filter

Click **Change Filter** to display the Search APs dialog box (see the following figure) and to create or change filter parameters. Click **Clear Filter** to remove the filter and display the entire access point list.

You can create a filter to display the list of access point by MAC address or AP name.

The following filter parameters are displayed in the Current Filter field.

- MAC Address—MAC address.
- AP Name—Access point name.
- CleanAir Oper Status—Operational status of the CleanAir capable access point. Choose from the following available statuses:
  - UP
  - DOWN
  - ERROR
  - N/A

Note When you enable filtering by the MAC address, the other filters are disabled automatically. However, you can use a combination of the AP Name and CleanAir Oper Status to filter access points.

Click **Find** to commit your changes. Only the access points that match your search criteria appear on the 802.11b/g/n Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

Note If you want to remove the filter and display the entire access point list, click **Clear Filter**.

802.11b/g/n Radios

To access details for each Cisco Radio, click the **Detail** link (see Radio Statistics for more information).

To access details of the air quality, click the blue arrow adjacent the desired access point radio and choose **CleanAir** (see Cisco CleanAir for more information).

Table 2-4 802.11b/g/n Radio Parameters

Parameters	Description
AP Name	Name assigned to the access point.
Radio Slot #	Slot where the radio is installed.
Base Radio MAC	MAC address of the access point.
Operational Status	Operational status of the Cisco Radios: UP or DOWN.
Load Profile	Radio Resource Management (RRM) profile for the Cisco Radio. The profile status is displayed as a pass or fail with details provided on the Radio Statistics data page.
Noise Profile	
Interference Profile	
Coverage Profile	
CleanAir Admin Status	Status of the CleanAir admin.
CleanAir Oper Status	Status of the spectrum sensor for this access point.

CleanAir Radio Monitoring Rapid Update

Choose **MONITOR > Access Points > Radios > 802.11a/n/ac** or **802.11b/g/n.** Click the blue arrow adjacent the desired access point radio and choose **CleanAir**. The 802.11a/n/ac (or 802.11b/g/n) > *Access Point Name* > Radio Monitoring Rapid Update page appears.

The Radio Monitoring Rapid Update page displays the CleanAir statistics for the selected Cisco Radio. You can alternate between the Graphics View and the Text View by clicking the **Graphics View/Text View** button. You can view and refresh the following statistics by selecting them (using the check boxes) and then clicking the **Refresh** button on the data page.

Active Interferer Parameters

Table 2-5 Active Interferer Parameters

Parameter	Description
Interferer Type	Type of the interferer.
Affected Channel	Channel that the device affects.
Detected Time	Time at which the interference was detected.
Severity	Severity index of the interfering device.
Duty Cycle (%)	Proportion of time during which the interfering device was active.
RSSI (dBm)	Receive signal strength indicator (RSSI) of the access point.
DevID	Device identification number that uniquely identifies the interfering device.
ClusterID	Cluster identification number that uniquely identifies the type of the devices.

Air Quality

The air quality provides a graphical representation of the average air quality for the access point on this radio.

Non-Wi-Fi Channel Utilization

The non-Wi-Fi channel utilization provides a graphical representation of the non-Wi-Fi channel utilization. The graph displays the percentage of spectrum used by the interference source.

Interference Power

The interference power provides a graphical representation of the non-Wi-Fi based interference source and displays the power level of the channel being affected.

Dual-Band Radios

Choose **MONITOR > Access Points > Radios > Dual-Band** to navigate to the Dual-Band Radios page.

This page displays the Cisco Radio profile and summary for your 802.11a/b/g/n RF network.

AP List Filter

Click **Change Filter** to display the Search APs dialog box (see the following figure) and to create or change filter parameters. Click **Clear Filter** to remove the filter and display the entire access point list.

You can create a filter to display the list of access point by MAC address or AP name.

The following filter parameters are displayed in the Current Filter field.

- MAC Address—MAC address.
- AP Name—Access point name.
- CleanAir Oper Status—Operational status of the CleanAir capable access point. Choose from the following available statuses:
  - UP
  - DOWN
  - ERROR
  - N/A

Note When you enable filtering by the MAC address, the other filters are disabled automatically. However, you can use a combination of the AP Name and CleanAir Oper Status to filter access points.

Click **Find** to commit your changes. Only the access points that match your search criteria appear on the Dual-Band Radio page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

Note If you want to remove the filter and display the entire access point list, click **Clear Filter**.

Dual-Band Radios Summary

Table 2-6 Dual-Band Radio Parameters

Parameters	Description
AP Name	Name assigned to the access point.
Radio Slot #	Slot where the radio is installed.
Base Radio MAC	MAC address of the access point.
Operational Status	Operational status of the Cisco Radios: UP or DOWN.
Load Profile	Radio Resource Management (RRM) profile for the Cisco Radio. The profile status is displayed as a pass or fail with details provided on the Radio Statistics data page.
Noise Profile	
Interference Profile	
Coverage Profile	
CleanAir Admin Status	Status of the CleanAir admin.
CleanAir Oper Status	Status of the spectrum sensor for this access point.

Cisco CleanAir

Choose **Monitor > Cisco CleanAir** to view the Interference Devices or the Air Quality Report pages. From here, you can choose the following:

- **MONITOR > Cisco CleanAir > 802.11 a/n/ac** (or **802.11 b/g/n**) > **Interference Devices** to view the the list of the interference devices in your 802.11a/n/ac or 802.11b/g/n RF network. See Cisco CleanAir Interference Devices for more information.
- **MONITOR > Cisco CleanAir > 802.11 a/n/ac** or **802.11 b/g/n** > **Air Quality Report**. to view the air quality of both the 802.11a/n/ac and 802.11b/g/n radio bands. See Cisco CleanAir Air Quality Report for more information.

Cisco CleanAir Interference Devices

Choose **Monitor > Cisco CleanAir > 802.11 a/n/ac** (or **802.11 b/g/n**) > **Interference Devices** to navigate to the Cisco CleanAir Interference Devices page. This page displays the list of the interference devices.

Table 2-7 Interference Device Parameters

Parameter	Description
AP Name	Name of the access point where the interference device is detected.
Radio Slot #	Slot that detects the interferers.
Device Type	Type of the device.
Affected Channel	Channel that the device affects.
Detected Time	Time at which the interference was detected.
Severity	Severity index of the interfering device.

Table 2-7 Interference Device Parameters

Parameter	Description
Duty Cycle (%)	Proportion of time during which the interfering device was active.
RSSI	Receive signal strength indicator (RSSI) of the access point.
DevID	Device identification number that uniquely identifies the interfering device.
ClusterID	Cluster identification number that uniquely identifies the type of the devices. When a CleanAir-enabled access point detects interference devices, these detections of the same device from multiple sensors are merged together to create clusters. Each cluster is given a unique ID. Some devices conserve power by limiting the transmit time until actually needed, which causes the spectrum sensor to temporarily stop detecting the device. This device is then correctly marked as down. A down device is removed from the spectrum database. In cases when all the interferer detections for a specific device are reported, the cluster ID is kept alive for an extended period of time to prevent possible device detection bouncing. If the same device is detected again, it is merged to the original cluster ID and the device detection history is preserved. For example, some Bluetooth headsets operate on battery power. These devices employ methods to reduce power consumption such as turning off the transmitter when it is not actually needed. Such devices can appear to come and go from the classification. To manage these devices, CleanAir keeps the cluster IDs longer and merges them again into a single record upon detection. Preventing bouncing smoothens the interference device records and allows the records to accurately represent the device history.

Click **Change Filter** to display the information about interference devices based on a particular criteria. Click **Clear Filter** to remove the filter and display entire access point list.

You can create a filter to display the list of interference devices that are based on the following filtering parameters:

- Cluster ID—To filter based on the Cluster ID, select the check box and enter the Cluster ID in the text box next to this field.

Note When a CleanAir-enabled access point detects interference devices, detections of the same device from multiple sensors are merged together. Each cluster is given a unique ID. Some devices conserve power by limiting the transmit time until actually needed, which allows the spectrum sensor to temporarily stop detecting the device. The device is then marked as down. A down device would be correctly removed from the spectrum database. In cases when all the interferer detections for a specific device are reported down, the cluster is kept alive for an extended period of time to prevent possible device detection bouncing. If the same device is detected again, it is merged to the original cluster and all the device history over time is kept together. For example, some Bluetooth headsets operate on battery power. These devices employ a power saving mode such as turning off the transmitter when it is not actually needed. Such devices can appear up and down. Bouncing prevention smoothens the interferer device records and accurately represents the device history.

- AP Name—To filter based on the access point name, select the check box and enter the access point name in the text box next to this field.

- Interferer Type—To filter based on the type of the interference device, select the check box and select the interferer device from the options.

  Select one of the following interferer devices:

  - TDD Transmit
  - Jammer
  - Continuous TX
  - DECT Phone
  - Video Camera
  - WiFi Inverted
  - WiFi Inv. Ch
  - SuperAG
  - Canopy
  - WiMax Mobile
  - WiMax Fixed
  - WiFi ACI
  - Unclassified
- Affected Channels
- Severity
- Duty Cycle (%)
- RSSI

Click **Find** to commit your changes.

The current filter parameters are displayed in the Current Filter field.

Cisco CleanAir > 802.11b/g/n > BLE Beacons

Choose **Monitor > Cisco CleanAir > 802.11 b/g/n > BLE Beacons** to navigate to the **802.11b/g/n Cisco APs > BLE Beacons** page, which shows the following details:

- AP Name
- Radio Slot#
- Device Type
- Affected Channel
- Detected Time
- Severity
- Duty Cycle(%)
- RSSI
- DevID
- Cluster ID

Cisco CleanAir Air Quality Report

Choose **Monitor > Cisco CleanAir > 802.11 a/n/ac** or **802.11 b/g/n > Air Quality Report** to navigate to the Air Quality Report page. This page displays the air quality on the access points. Air Quality is checked on all channels if you have a monitor module for an Cisco Aironet 3600 series access point.

Table 2-8 Cisco CleanAir Air Quality Report Parameters

Parameter	Description
AP Name	Name of the access point.
Radio Slot #	Slot where the interference is detected.
Channel	Channel where the air quality is monitored.
Average AQ	Average air quality observed.
Minimum AQ	Minimum air quality observed.
Interferer	Number of devices that affect a particular channel.
DFS (Dynamic Frequency Selection)	Whether DFS is enabled.

Cisco CleanAir Worst Air Quality Report

Choose **Monitor > Cisco CleanAir > Worst Air Quality Report**. to navigate to the the Worst Air Quality Report page. This page shows the air quality of both the 802.11a/n/ac and 802.11b/g/n radio bands.

Table 2-9 Cisco CleanAir Worst Air Quality

Parameter	Description
AP Name	Name of the access point that reported the worst air quality for the 802.11a/n/ac or 802.11b/g/n radio band.
Channel Number	Radio channel with the worst reported air quality.
Minimum Air Quality Index (1 to 100)	Minimum air quality for this radio channel. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
Average Air Quality Index (1 to 100)	Average air quality for this radio channel. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
Interference Device Count	Number of interferers detected by the radios on the 802.11a/n/ac or 802.11b/g/n radio band.

To view a list of persistent sources of interference for a specific access point radio, follow these steps:

Step 1 **Choose Wireless > Access Points > Radios > 802.11a/n/ac** or **802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.

Step 2 Click the blue arrow adjacent the desired access point radio and choose **CleanAir-RRM**. The 802.11a/n/ac (or 802.11b/g/n) Cisco APs > *Access Point Name* > Persistent Devices page appears.

This page lists the device types of persistent sources of interference detected by this access point radio. It also shows the channel on which the interference was detected, the percentage of time that the interferer was active (duty cycle), the received signal strength (RSSI) of the interferer, and the day and time when the interferer was last detected.

Statistics

Choose **MONITOR > Statistics** to navigate to the Statistics page. From here, you can choose the following:

- **MONITOR > Statistics > Controller** to view the controller statistics.

  See Controller Statistics for more information.
- **MONITOR > Statistics > AP Join** to view all the access points that have joined or have tried to join to the controller.

  See AP Join Statistics for more information.
- **MONITOR > Statistics > Port** to view the status of each port on the controller.

  See Port Statistics for more information.
- **MONITOR > Statistics > RADIUS Servers** to view addressing and status information of your RADIUS servers.

  See RADIUS Server Statistics for more information.
- **MONITOR > Statistics > Mobility Statistics** to view the statistics for mobility group events.

  See Mobility Statistics for more information.
- **MONITOR > Statistics > IPv6 Neighbor Bind Counters** to view counter statistics for the following Neighbor Discovery Protocol (NDP) and Dynamic Host Configuration Protocol (DHCP) packets.

  See IPv6 Neighbor Bind Counters for more information.
- **MONITOR > Statistics > PMIPv6 LMA Statistics** to view the statistics of all the LMA (Local Mobility Anchor) that the controller is connected to.

  See PMIPv6 LMA Statistics for more information.
- **MONITOR > Statistics > Preferred Mode Statistics** to view the details of the APs on which the IP config (Global/ AP Group) has been configured.

  See Preferred Mode for more information.
- **MONITOR > Statistics > Optimized Roaming** to view the details of optimized roaming.

Controller Statistics

Choose **MONITOR > Statistics > Controller** to view the controller statistics.

Note All the statistics related to received packets are Ethernet packets received on the controller port . These packets are a combination of CAPWAP packets, and packets from any wired infrastructure that reach the controller.
All the statistics related to packets transmitted from the controller include CAPWAP packets to access points and non-encapsulated packets to wired infrastructure.

Table 2-10 Controller Summary Statistics

Parameter	Description
Octets Received	Total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Packets Received Without Error	Total number of packets received by the processor.
Unicast Packets Received	Number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	Total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	Total number of packets received that were directed to the broadcast address.
Receive Packets Discarded	Number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their delivery to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted	Total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted without Errors	Total number of packets transmitted out of the interface.
Unicast Packets Transmitted	Total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those packets that were discarded or not sent.
Multicast Packets Transmitted	Total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	Number of packets that higher-level protocols requested be transmitted to the broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	Number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their delivery to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Most Address Entries Ever Used	Highest number of Forwarding Database Address Table entries that have been learned by this controller since the most recent reboot.
Address Entries in Use	Number of learned and static entries in the Forwarding Database Address Table for this controller.

Table 2-10 Controller Summary Statistics

Parameter	Description
Maximum VLAN Entries	Maximum number of Virtual LANs (VLANs) allowed on this controller.
Most VLAN Entries Ever Used	Largest number of VLANs that have been active on this controller since the last reboot.
Static VLAN Entries	Number of presently active VLAN entries on this controller that have been created statically.
Time Since Counters Last Cleared	Elapsed time, in days, hours, minutes, and seconds, since the statistics for this controller were last cleared.

Click **Clear Counters** to set all summary and detailed controller statistics counters to zero; also resets the Time Since Counters Last Cleared field.

AP Join Statistics

Choose **MONITOR > Statistics > AP Join** to navigate to the AP Join Statistics page.

The join statistics for an access point that send a CAPWAP discovery request to the controller at least once are maintained on the controller even if the access point is rebooted or disconnected. These statistics are removed only if the controller is rebooted or if you choose to clear the statistics.

This page lists all of the access points that are joined to the controller or that have tried to join. It shows the radio MAC address, access point name, current join status, Ethernet MAC address, IP address, and last join time for each access point.

The total number of access points appears in the upper right-hand corner of the page. If the list of access points spans multiple pages, you can access these pages by clicking the page number links. Each page shows the join statistics for up to 25 access points.

AP List Filter

Click **Change Filter** to display the Search APs dialog box (see the following figure) and to create or change filter parameters. Click **Clear Filter** to remove the filter and display the entire access point list.

You can create a filter to display the list of access point by MAC address or AP name.

The following filter parameters are displayed in the Current Filter field.

- **Ethernet MAC Address—**MAC address.
- **AP Name—**Access point name.

Note When you enable one of these filters, the other filter is disabled automatically.

Click **Find** to commit your changes. Only the access points that match your search criteria appear on the AP Join Stats page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC Address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

Note If you want to remove the filter and display the entire access point list, click **Show All**.

Click the MAC address of the radio to see detailed statistics for each port on the AP Join Stats Detail page (see AP Join Statistics Detail for more information).

To remove an access point from the list, click the blue arrow adjacent the desired access point and choose **Remove**.

Click **Clear Stats on All APs** to clear the statistics for all access points.

AP Join Statistics Detail

Choose **MONITOR > Statistics > AP Join** and then click the base radio MAC address to navigate to the **AP Join Stats Detail** page. This page provides information on each phase of the join process and shows any errors that have occurred.

Port Statistics

Choose **MONITOR > Statistics > Ports** to navigate to the Ports Statistics page. This page displays the status of each port on the controller. This table describes the ports statistics parameters.

Table 2-11 Summary Parameters

Parameter	Description	Range
Port No	Port number on the controller.	1–12 for 10/100BASE-T, 13 for 1000BASE-T or 1000BASE-SX. 1–24 for 10/100BASE-T, 25 for 1000BASE-T or 1000BASE-SX. 1 for 1000BASE-SX on a Cisco 4100 Series Wireless LAN Controller. 1 for 1000BASE-SX on a Cisco 4100 Series Wireless LAN Controller.
Admin Status	State of the port.	Enable or Disable.
Physical Mode	Configuration of the port physical interface.	Auto. 100 Mbps full duplex. 100 Mbps half duplex. 10 Mbps full duplex. 10 Mbps half duplex. 1000 Mbps full duplex. **Note** In a Cisco NMWLC6 controller, the physical mode is always set to Auto.

Table 2-11 Summary Parameters

Parameter	Description	Range
Physical Status	Actual port physical interface.	Auto. 100 Mbps full duplex. 100 Mbps half duplex. 10 Mbps full duplex. 10 Mbps half duplex. 1000 Mbps full duplex.
Link Status	Displays the status of the link.	Link Up or Link Down.

The Physical Mode and Status may reflect different values depending on the link status. For example, the Physical Mode may be set to Auto while the link actually runs at 10 Mbps half duplex.

Ports Statistics Details

Choose **MONITOR > Statistics > Ports** and then click **View Stats** to view the port details.

Table 2-12 Port Statistics

Parameter	Received Description	Transmitted Description
Total Bytes	Total number of octets of data (including those octets in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value Utilization which is the percentage of utilization of the Ethernet segment on a scale of 0 to 100 percent.	Number of octets of data (including those octets in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets (64 Octets)	Total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).	Total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
Packets (65-127 Octets)	Total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).	Total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

Table 2-12 Port Statistics

Parameter	Received Description	Transmitted Description
Packets (128-255 Octets)	Total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).	Total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets (256-511 Octets)	Total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).	Total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets (512-1023 Octets)	Total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).	Total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets (1024-1518 Octets)	Total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).	Total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets (> 1518 Octets)	Total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.	Total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

Maximum Info size allowed—The maximum size of the Info (non-MAC) field that this port receives or transmits.

Table 2-13 Successful Packets

Parameter	Received Description	Transmitted Description
Total	Total number of packets received that were without errors.	Total number of packets transmitted that were without errors.
Unicast Packets	Number of subnetwork-unicast packets delivered to a higher-layer protocol.	Total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those packets that were discarded or not sent.

Table 2-13 Successful Packets

Parameter	Received Description	Transmitted Description
Multicast Packets	Total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.	Total number of packets that higher-level protocols requested be transmitted to a multicast address, including those packets that were discarded or not sent.
Broadcast Packets	Total number of good packets received that were directed to the broadcast address.	Total number of packets that higher-level protocols requested be transmitted to the broadcast address, including those packets that were discarded or not sent.

Table 2-14 Protocol Statistics

Parameter	Received Description	Transmitted Description
802.3x Pause Frames Received	Media Access Control (MAC) frames received on this interface with an opcode indicating a PAUSE. This counter does not increment when the interface operates in half-duplex mode.	–

Time Since Counters Last Cleared—The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

Click **Clear Counters** to set all summary and controller detailed statistics counters to zero and to reset the "Time Since Counters Last Cleared" field.

Table 2-15 Received Packets with MAC Errors Parameters

Parameter	Description
Total	Total number of inbound packets that contained errors preventing them from delivery to a higher-layer protocol.
Jabbers	Number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). This definition of jabber differs from the definition in IEEE 802.3, section 8.2.1.5 (10BASE-5) and section 10.3.1.4 (10BASE-2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
Fragments/ Undersize	Number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
Alignment Errors	Number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a nonintegral number of octets.

Table 2-15 Received Packets with MAC Errors Parameters

Parameter	Description
FCS Errors	Number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.
Overruns	Number of frames discarded because this port was overloaded with incoming packets and could not keep up with the inflow.

Table 2-16 Details of Received Packets Not Forwarded

Parameter	Description
Total	Count of valid frames received that were discarded or filtered by the forwarding process.
Local Traffic Frames	Total number of dropped frames in the forwarding process because the destination address was located off of this port.
802.3x Pause Frames Received	Count of MAC control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface operates in half-duplex mode.
Unacceptable Frame Type	Number of frames discarded from this port due to unacceptable frame types.
VLAN Membership Mismatch	Number of frames discarded on this port due to ingress filtering.
VLAN Viable Discards	Number of frames discarded on this port because a lookup on a particular VLAN occurred while that entry in the VLAN table was modified, or if the VLAN had not been configured.
Multicast Tree Viable Discards	Number of frames discarded because a lookup in the multicast tree for a VLAN occurred while that tree was modified.
Reserved Address Discards	Number of frames discarded that were destined to an IEEE 802.1 reserved address and were not supported by the system.
CFI Discards	Number of frames discarded that had the CFI bit set and the addresses in RIF were in noncanonical format.
Upstream Threshold	Number of frames discarded due to a lack of cell descriptors available for that packet's priority level.

Table 2-17 Transmit Error Parameters

Parameter	Description
Total Errors	Sum of Single, Multiple, and Excessive Collisions.
FCS Errors	Total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.

Table 2-17 Transmit Error Parameters

Parameter	Description
Oversized	Number of frames that exceeded the maximum permitted frame size. This counter has a maximum increment rate of 815 counts per second at 10 Mbps.
Underrun Errors	Number of frames discarded because the transmit FIFO buffer became empty during the frame transmission.

Table 2-18 Transmit Discard Parameters

Parameter	Description
Total Discards	Sum of discarded single collision frames, discarded multiple collision frames, and discarded excessive frames.
Single Collision Frames	Count of the number of successfully transmitted frames on a particular interface for which transmission was inhibited by one collision.
Excessive Collisions	Count of frames for which transmission on a particular interface failed due to excessive collisions.
Port Membership	Number of frames discarded on egress for this port due to egress filtering being enabled.
VLAN Viable Discards	Number of frames discarded on this port because a lookup on a particular VLAN occurred while that entry in the VLAN table was modified, or if the VLAN had not been configured.
Multiple Collision Frames	Count of the number of successfully transmitted frames on a particular interface for which transmission was inhibited by more than one collision.

RADIUS Server Statistics

Choose **MONITOR > Statistics > RADIUS Servers** to navigate to the **RADIUS Servers** page.

This page displays addressing and status information for your Remote Authentication Dial-In User Servers (RADIUS). Configure the authentication and accounting servers by choosing the Security tab from the menu bar.

Table 2-19 Authentication Server and Accounting Server Status Parameters

Parameter	Description
Index	Access priority number for RADIUS servers. Up to 17 authentication and 17 accounting servers can be configured. The controller polling of the servers starts with Index 1, Index 2 second, and so forth. The index number is based on the server index priority that is selected for a RADIUS server when it is added to the controller.
Address	IP address of the RADIUS server.
Port	Communication port.
Admin Status	Enabled or disabled.

RADIUS Servers Authentication Statistics

Choose **MONITOR > Statistics > RADIUS Servers** and then click **Stats** in a RADIUS Authentication entry to navigate to the RADIUS Server Authentication Stats page.

This page displays addressing and status information for your RADIUS servers.

Authentication Server Addressing

Table 2-20 Authentication Server Addressing Parameters

Parameter	Description
Server Index	Access priority number for RADIUS servers. Up to 17 servers can be configured. The controller polling of the servers starts with Index 1 first, Index 2 second, and so on. The index number is based on the server index priority that is selected for a RADIUS server when it is added to the controller.
Server Address	IP address of the RADIUS server.
Admin Status	State of the server.

Authentication Server Statistics

Table 2-21 Authentication Server Statistics Parameters

Parameter	Description
Msg Round Trip Time	Time interval between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
First Requests	Number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Retry Requests	Number of RADIUS Authentication-Request packets retransmitted to this RADIUS authentication server.
Accept Responses	Number of RADIUS Access-Accept packets (valid or invalid) received from this server.
Reject Responses	Number of RADIUS Access-Reject packets (valid or invalid) received from this server.
Challenge Responses	Number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
Malformed Messages	Number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators, signature attributes, or unknown types are not included as malformed access responses.
Bad Authenticator Msgs	Number of RADIUS Access-Response packets that contain invalid authenticators or signature attributes received from this server.
Pending Requests	Number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, a timeout, or retransmission.

Table 2-21 Authentication Server Statistics Parameters

Parameter	Description
Timeout Requests	Number of authentication timeouts to this server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
Unknown Type Msgs	Number of RADIUS packets of unknown type received from this server on the authentication port.
Other Drops	Number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

RADIUS Servers Accounting Statistics

Choose **MONITOR > Statistics > RADIUS Servers** and then click **Stats** in a RADIUS Accounting entry to navigate to the RADIUS Servers Accounting Stats page.

This page displays addressing and status information for your Remote Authentication Dial-In User Servers.

Accounting Server Addressing

Table 2-22 Accounting Server Addressing Parameters

Parameter	Description
Server Index	Access priority number for RADIUS servers. Up to 17 servers can be configured. The controller polling of the servers starts with Index 1 first, Index 2 second, and so on. The index number is based on the server index priority that is selected for a RADIUS server when it is added to the controller.
Server Address	IP address of the RADIUS server.
Admin Status	State of the server.

Accounting Server Statistics

Table 2-23 Accounting Server Statistics Parameters

Parameter	Description
Msg Round Trip Time	Time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
First Requests	Number of RADIUS Accounting-Request packets sent. This number does not include retransmissions.
Retry Requests	Number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Accounting Responses	Number of RADIUS packets received on the accounting port from this server.

Table 2-23 Accounting Server Statistics Parameters

Parameter	Description
Malformed Messages	Number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticator Msgs	Number of RADIUS Accounting-Response packets that contained invalid authenticators received from this server.
Pending Requests	Number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout, or a retransmission.
Timeout Requests	Number of accounting timeouts to this server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
Unknown Type Msgs	Number of RADIUS packets of unknown type received from this server on the accounting port.
Other Drops	Number of RADIUS packets that were received from this server on the accounting port and dropped for some other reason.

Mobility Statistics

Choose **MONITOR > Statistics > Mobility Statistics** to navigate to the Mobility Statistics page.

This page displays the statistics for mobility group events and is divided into the following three groups:

- Global Statistics that affect all mobility transactions.
- Mobility Initiator Statistics generated by the controller that initiates the mobility event.
- Mobility Responder Statistics generated by the controller that responds to a mobility event.

Global Mobility Statistics

Table 2-24 Global Mobility Statistics Parameters

Parameter	Description
Rx Errors	Generic protocol packet receive errors (such as the packet was too short or format was incorrect).
Tx Errors	Generic protocol packet transmit errors, such as the packet transmission failed.
Responses Retransmitted	Number of retransmitted responses. The mobility protocol uses UDP and it resends requests several times if it does not receive a response. Because of network or processing delays, the responder may receive one or more retry requests after it initially responds to a request. This count includes the response resends.

Table 2-24 Global Mobility Statistics Parameters

Parameter	Description
Handoff Requests Received	Number of handoff requests received, ignored, or responded.
Handoff End Requests Received	Total number of handoff end requests received. These requests are sent by the anchor or the foreign controller to notify the other about the close of a client session.
State Transitions Disallowed	Number of disallowed state transitions. PEM (policy enforcement module) has denied a client state transition, which results in an aborted handoff.
Resource Unavailable	Unavailable resource, such as a buffer, which resulted in an aborted handoff.

Mobility Initiator Statistics

Table 2-25 Mobility Initiator Statistics

Parameter	Description
Handoff Requests Sent	Number of clients that have associated with the controller and have been announced to the mobility group.
Handoff Replies Received	Number of handoff replies that have been received in response to the requests sent.
Handoff as Local Received	Number of handoffs in which the entire client session has been transferred.
Handoff as Foreign Received	Number of handoffs in which the client session was anchored elsewhere.
Handoff Denys Received	Number of handoffs that were denied.
Anchor Request Sent	Number of anchor requests that were sent for a three party (foreign to foreign) handoff. The handoff was received from another foreign controller and the new controller is requesting the anchor controller to move the client.
Anchor Deny Received	Number of anchor requests that were denied by the current anchor.
Anchor Grant Received	Number of anchor requests that were approved by the current anchor.
Anchor Transfer Received	Number of anchor requests that closed the session on the current anchor and transferred the anchor back to the requestor.

Mobility Responder Statistics

Table 2-26 Mobility Responder Statistics

Parameter	Description
Handoff Requests Ignored	Number of handoff requests/client announcements that were ignored. The controller had no knowledge of that client.
Ping Pong Handoff Requests Dropped	Number of handoff requests that were denied because the handoff period was too short (3 seconds).
Handoff Requests Dropped	Number of handoff requests that were dropped due to a either an incomplete knowledge of the client or a problem with the packet.
Handoff Requests Denied	Number of handoff requests that were actively denied.
Client Handoff as Local	Number of handoffs responses sent while in the local role.
Client Handoff as Foreign	Number of handoffs responses sent while in the foreign role.
Anchor Requests Received	Number of anchor requests received.
Anchor Requests Denied	Number of anchor requests denied.
Anchor Requests Granted	Number of anchor requests granted.
Anchor Transferred	Number of anchors transferred because the client moved from a foreign controller to a controller on the same subnet as the current anchor.

IPv6 Neighbor Bind Counters

Choose **MONITOR > Statistics > IPv6 Neighbor Bind Counters** to navigate to the IPv6 Neighbor Bind Counters page.

This page displays counter statistics for the following Neighbor Discovery Protocol (NDP) and Dynamic Host Configuration Protocol (DHCP) packets:

- Received Messages
- Bridged Messages
- Dropped Messages
- NDSUPRRESS Drop counters
- SNOOPING Drop counters

Received Messages

Table 2-27 Received Message Statistics

Parameter	Description
NDP Router Solicitation	Number of received messages originated by the hosts to request a router to send a router advertisement.
NDP Router Advertisement	Number of received messages originated by the routers to advertise their presence and link-specific parameters such as link prefixes, link MTU, and hop limits. These messages are sent periodically and also in response to router solicitation messages.
NDP Neighbor Solicitation	Number of received messages originated by the nodes to request the link layer address of another node and also for functions such as duplicate address detection and neighbor unreachability detection.
NDP Neighbor Advertisement	Number of received messages in response to neighbor solicitation messages. If a node changes its link-layer address, it can send an unsolicited neighbor advertisement to advertise the new address.
NDP Redirect	Number of received messages to inform a host of a better first-hop node on the path to a destination. Hosts can be redirected to a better first-hop router but can also be informed by a redirect that the destination is in fact a neighbor.
NDP Certificate Solicit	Number of received messages to know the certification path to the trust anchor. Hosts will send the Certification Path Solicitations.
NDP Certificate Advert	Number of received messages to know the certification path to the trust anchor. Routers will send the Certification Path Advertisement messages.
DHCPv6 Solicitation	Number of received messages sent by a client to locate DHCPv6 servers.
DHCPv6 Advertisement	Number of received messages sent by a DHCPv6 server in response to a DHCPv6 solicitation message to indicate availability.
DHCPv6 Request	Number of received messages sent by a client to request addresses or configuration settings from a server.
DHCPv6 Reply	Number of received messages sent by a DHCPv6 server to a client in response to a Solicit, Request, Renew, Rebind, Information-Request, Confirm, Release, or Decline message.
DHCPv6 Inform	Number of received messages sent by a client to request configuration settings (but not addresses).
DHCPv6 Confirm	Number of received messages sent by a client to all servers to determine if a client's configuration is valid for the connected link.

Table 2-27 Received Message Statistics

Parameter	Description
DHCPv6 Renew	Number of received messages sent by a client to a server to extend the lifetime of assigned addresses and obtain updated configuration settings.
DHCPv6 Rebind	Number of received messages sent by a client to any server when a response to the DHCPv6 Renew message is not received.
DHCPv6 Release	Number of received messages sent by a server to a client in response to a Solicit, Request, Renew, Rebind, Information-Request, Confirm, Release, or Decline message.
DHCPv6 Decline	Number of received messages sent by a client to a server to indicate that the assigned address is already in use.
DHCPv6 Reconfigure	Number of received messages sent by a server to a client to indicate that the server has new or updated configuration settings.
DHCPv6 Relay Forward	Number of received messages sent by a relay agent to forward a message to a server. Contains a client message encapsulated as the DHCPv6 Relay-Message option.
DHCPv6 Relay Reply	Number of received messages sent by a server to send a message to a client through a relay agent. Contains a server message encapsulated as the DHCPv6 Relay-Message option.

Bridged Messages

Table 2-28 Bridged Message Statistics

Parameter	Description
NDP Router Solicitation	Number of received bridged messages originated by the hosts to request a router to send a router advertisement.
NDP Router Advertisement	Number of received bridged messages originated by the routers to advertise their presence and link specific parameters such as link prefixes, link MTU, and hop limits. These messages are sent periodically and also in response to Router Solicitation messages.
NDP Neighbor Solicitation	Number of received bridged messages originated by the nodes to request another node's link layer address and also for functions such as duplicate address detection and neighbor unreachability detection.
NDP Neighbor Advertisement	Number of received bridged messages in response to Neighbor Solicitation messages. If a node changes its link-layer address, it can send an unsolicited Neighbor Advertisement to advertise the new address.

Table 2-28 Bridged Message Statistics

Parameter	Description
NDP Redirect	Number of received bridged messages to inform a host of a better first-hop node on the path to a destination. Hosts can be redirected to a better first-hop router but can also be informed by a redirect that the destination is in fact a neighbor.
NDP Certificate Solicit	Number of received bridged messages to know the certification path to the trust anchor. Hosts will send the Certification Path Solicitations.
NDP Certificate Advert	Number of received bridged messages to know the certification path to the trust anchor. Routers will send the Certification Path Advertisement messages.
DHCPv6 Solicitation	Number of received bridged messages sent by a client to locate DHCPv6 servers.
DHCPv6 Advertisement	Number of received bridged messages sent by a DHCPv6 server in response to a DHCPv6 Solicitation message to indicate availability.
DHCPv6 Request	Number of received bridged messages sent by a client to request addresses or configuration settings from a server.
DHCPv6 Reply	Number of received bridged messages sent by a DHCPv6 server to a client in response to a Solicit, Request, Renew, Rebind, Information-Request, Confirm, Release, or Decline message.
DHCPv6 Inform	Number of received bridged messages sent by a client to request configuration settings (but not addresses).
DHCPv6 Confirm	Number of received bridged messages sent by a client to all servers to determine if a client's configuration is valid for the connected link.
DHCPv6 Renew	Number of received bridged messages sent by a client to a server to extend the lifetime of assigned addresses and obtain updated configuration settings.
DHCPv6 Rebind	Number of received bridged messages sent by a client to any server when a response to the DHCPv6 Renew message is not received.
DHCPv6 Release	Number of received bridged messages sent by a server to a client in response to a DHCPv6 Solicitation, Request, Renew, Rebind, Information-Request, Confirm, Release, or Decline message.
DHCPv6 Decline	Number of received bridged messages sent by a client to a server to indicate that the assigned address is already in use.
DHCPv6 Reconfigure	Number of received bridged messages sent by a server to a client to indicate that the server has new or updated configuration settings. The client then sends either a Renew or Information-Request message.

Table 2-28 Bridged Message Statistics

Parameter	Description
DHCPv6 Relay Forward	Number of received bridged messages sent by a relay agent to forward a message to a server. Contains a client message encapsulated as the DHCPv6 Relay-Message option.
DHCPv6 Relay Reply	Number of received bridged messages sent by a server to send a message to a client through a relay agent. Contains a server message encapsulated as the DHCPv6 Relay-Message option.

Dropped Messages

Table 2-29 Dropped Message Statistics

Parameter	Description
NDP RS Drop (Router Solicitation)	Number of messages dropped that are originated by the hosts to request a router to send a Router Advertisement.
NDP RA Drop (Router Advertisement)	Number of messages dropped that are originated by the routers to advertise their presence and link-specific parameters such as link prefixes, link MTU, and hop limits. These messages are sent periodically and also in response to Router Solicitation messages.
NDP NS Drop (Neighbor Solicitation)	Number of messages dropped that are originated by the nodes to request another node's link layer address and also for functions such as duplicate address detection and neighbor unreachability detection.
NDP NA Drop (Neighbor Advertisement)	Number of messages dropped in response to Neighbor Solicitation messages. If a node changes its link-layer address, it can send an unsolicited Neighbor Advertisement to advertise the new address.
DHCPv6 Solicitation	Number of messages dropped that are sent by a client to locate DHCPv6 servers.
DHCPv6 Advertisement	Number of messages dropped that are sent by a DHCPv6 server in response to a DHCPv6 Solicitation message to indicate availability.
DHCPv6 Reply	Number of messages dropped that are sent by a DHCPv6 server to a client in response to a Solicit, Request, Renew, Rebind, Information-Request, Confirm, Release, or Decline message.
DHCPv6 Inform	Number of messages dropped that are sent by a client to request configuration settings (but not addresses).

NDSUPRRESS Drop Counters

Table 2-30 NDSUPRESS Drop Counter Statistics

Parameter	Description
total	Total number of NDSUPRESS dropped messages.
silent	Number of silently dropped messages.
ns_in_out	Number of Neighbor Solicitation (NS) owner messages on the input interface.
ns_dad	Number of NS Duplicate Address Detection (DAD) messages suppressed.
unicast	Number of NS unicast messages suppressed.
multicast	Number of NS multicast messages suppressed.
internal	Number of internal failure messages.

SNOOPING Drop Counters

Table 2-31 SNOOPING Drop Counter Statistics

Parameter	Description
Dropped Messages	Name of the dropped messages.
total	Total number of dropped messages.
silent	Number of silently dropped messages.
internal	Number of internal failure messages.
CGA_vfy	Number of messages where Cryptographically Generated Address (CGA) option is not getting verified.
RSA_vfy	Number of messages where RSA signature is not getting verified.
limit	Number of messages in which the address limit is reached.
martian	Number of Martian packets. A Martian packet is an IP packet which specifies a source or destination address that is reserved for special-use by Internet Assigned Numbers Authority (IANA) and cannot actually originate as claimed or be delivered. Martian packets commonly arise from IP address spoofing in denial-of-service attacks, but can also arise from network equipment malfunction or misconfiguration of a host.
martian_mac	Number of Martian MAC packets.
no_trust	Number of packets marked for detection of policy and collision.

Table 2-31 SNOOPING Drop Counter Statistics

Parameter	Description
not_auth	Number of packets that are not authorized on port.
stop	Number of packets that are accepted, but not forwarded.

CacheMiss Statistics

Table 2-32 CacheMiss Statistics

Parameter	Description
Multicast NS Forwarded	Total number of NS-forwarded multicast messages.
Multicast NS Dropped	Total number of NS-dropped multicast messages.

Click **Clear Count** to set all IPv6 Neighbor Bind Counter statistics to zero.

PMIPv6 LMA Statistics

Choose **MONITOR > Statistics > PMIPv6 LMA Statistics** to navigate to the PMIPv6 LMA Statistics page.

This page enables you to view the statistics of all the LMA (Local Mobility Anchor) that the controller is connected to. This table describes the LMA statistics.

Table 2-33 LMA Statistics

Parameter	Description
LMA Name	Name of the LMA.
Total Bindings	Total number of binding updates sent to the LMA by the controller.
PBU Sent	Total number of Proxy Binding Updates (PBUs) sent to the LMA by the controller. PBU is a request message sent by the Mobile Access Gateway (MAG) to a mobile node's LMA for establishing a binding between the mobile node's interface and its current care-of address (Proxy-CoA).
PBA Received	Total number of Proxy Binding Acknowledgements (PBAs) received by the controller for the LMA. PBA is a reply message sent by an LMA in response to a PBU message that it received from a MAG.
PBRI Sent	Total number of Proxy Binding Revocation Indications (PBRIs) sent by the controller to the LMA.

Table 2-33 LMA Statistics

Parameter	Description
PBRI Received	Total number of PBRIs received from the LMA by the controller.
PBRA Sent	Total number of Proxy Binding Revocation Acknowledgements (PBRAs) sent by the controller to the LMA.
PBRA Received	Total number of PBRAs received from the LMA by the controller.
Number of Handoff	Number of handoffs between the controller and the LMA.
PBU Dropped	Number of PBUs dropped between the controller and the LMA.

Preferred Mode

Choose **MONITOR > Statistics > Preferred Mode** to navigate to the Preferred Mode Statistics page.

This page enables you to view the details of the APs on which the IP config (Global/ AP Group) has been configured.

Table 2-34 Preferred Mode Statistics

Parameter	Description
Prefer Mode of Global/AP Groups	The name of the AP that is configured with either IPv4, IPv6 or global.
Total	The total count of APs configured with preferred mode.
Success	Counts the number of times the AP was successfully configured with the preferred mode.
Unsupported	The number of APs that are not supported with the controller.
Already Configured	Counts the attempts made to configure an already configured AP.
Per AP Group Configured	Preferred mode configured on per AP group
Failure	Counts the number of times the AP was failed to get configured with the preferred mode.

Optimized Roaming

Choose **MONITOR > Statistics > Optimized Roaming** to navigate to the **Optimized Roaming Statistics** page.

The **Optimized Roaming Statistics** page provides statistics related to disassociations and rejections on 802.11a and 802.11b radios.

Cisco Discovery Protocol

Choose **MONITOR > CDP** to navigate to the CDP page. From here, you can choose the following:

- **MONITOR > CDP > Interface Neighbors** to view a list of all CDP neighbors on all interfaces.
  See CDP Interface Neighbors for more information.
- **MONITOR > CDP > AP Neighbors** to view a all access points with CDP neighbors.
  See CDP AP Neighbors for more information.
- **MONITOR > CDP > Traffic Metrics** to display CDP traffic information.
  See CDP Traffic Metrics for more information.

CDP Interface Neighbors

Choose **MONITOR > CDP > Interface Neighbors** to navigate to the CDP Interface Neighbors page.

This page enables you to view a list of all Cisco Discovery Protocol neighbors on all interfaces.

This table describes the CDP interface neighbor parameters.

Table 2-35 CDP Interface Neighbor Parameters

Parameter	Description
Local Interface	Local interface name.
Neighbor Name	Name of each CDP neighbor.
Neighbor Address	IPv4 or IPv6 address of the CDP neighbor.
Neighbor Port	IP address of each CDP neighbor.
TTL	Time left (in seconds) before each CDP neighbor entry expires.
Capability	Functional capability of each CDP neighbor: • R—Router • T—Trans Bridge • B—Source Route Bridge • S—Switch • H—Host • I—IGMP • r—Repeater • M—Remotely Managed Device
Platform	CDP neighbor device platform.

CDP Interface Neighbors Details

Choose **MONITOR > CDP > Interface Neighbors**, and then click the neighbor name for the desired interface to view the CDP Interface Neighbors Details page. This page enables you to view detailed information about the Cisco Discovery Protocol neighbor of each interface.

Table 2-36 CDP Neighbor Detail Parameters

Parameter	Description
Local Interface	controller port on which the CDP packets were received.
Neighbor Name	Name of the CDP neighbor.
Neighbor Address	IPv4 or IPv6 address of the CDP neighbor.
Neighbor Port	Port used by the CDP neighbor for transmitting CDP packets.
Duplex	Duplex type of the CDP neighbor.
Advt Version	CDP version being advertised (v1 or v2).
TTL	Time left (in seconds) before the CDP neighbor entry expires.
Capability	Functional capability of the CDP neighbor: • Router • Trans Bridge • Source Route Bridge • Switch • Host • IGMP • Repeater • Remotely Managed Device
Platform	Hardware platform of the CDP neighbor device.
Software Version	Software running on the CDP neighbor.

CDP AP Neighbors

Choose **MONITOR > CDP > AP Neighbors** to navigate to the AP Neighbors page. This page enables you to view a list of all access points with CDP neighbors.

Table 2-37 CDP AP Neighbor Details

Parameter	Description
AP Name	Access point name.
CDP Neighbors	CDP neighbor name.

Click **CDP Neighbors** to view the CDP neighbors for the access points that are connected to the controller in the CDP Neighbors page.

CDP Neighbors

Choose **MONITOR > CDP > AP Neighbors** and then click **CDP Neighbors** for an access point to navigate to the CDP Neighbors page. This page enables you to view the CDP neighbors for the access points that are connected to the controller.

Table 2-38 AP Neighbor Parameters

Parameter	Description
AP Name	Access point name.
AP IP Address	IP address of the access point.
Neighbor Name	Name of the neighbor.
Neighbor Address	IP address of the neighbor.
Neighbor Port	Port number of the neighbor.
Advt Version	Advertised CDP version (v1 or v2).

CDP Neighbors Details

Choose **MONITOR > CDP > AP Neighbors**, and then click the access point name for the desired access point and view the CDP AP Neighbors Details page. This page enables you to view to see more detailed information about an access point's CDP neighbor.

The following AP neighbor details are displayed:

- AP Name—The name of the access point
- Basic Radio MAC—The MAC address of the access point's radio
- AP IP Address—The IP address of the access point
- Local Interface—The interface on which the CDP packets were received
- Neighbor Name—The name of the CDP neighbor
- Neighbor Address—The IPv4 and IPv6 address of the CDP neighbor
- Neighbor Port—The port used by the CDP neighbor
- Advt Version—The CDP version being advertised (v1 or v2)
- TTL—The time left (in seconds) before the CDP neighbor entry expires
- Capability—The functional capability of the CDP neighbor:
  - Router
  - Trans Bridge
  - Source Route Bridge
  - Switch
  - Host
  - IGMP
  - Repeater
  - Remotely Managed Device
- Platform—The hardware platform of the CDP neighbor device

- Software Version—The software running on the CDP neighbor

CDP Traffic Metrics

Choose **MONITOR > CDP > Traffic Metrics** to navigate to the CDP Traffic Metrics page. This page displays CDP traffic information.

Table 2-39 CDP Traffic Metrics

Parameter	Description
Packets In	Number of CDP packets received by the controller.
Packet Out	Number of CDP packets sent from the controller.
Checksum Errors	Number of packets that experienced a checksum error.
No Memory Errors	Number of packets dropped due to insufficient memory.
Invalid Packets	Number of invalid packets.

Rogues

Choose **MONITOR > Rogues** to navigate to the Rogues page. From here, you can choose the following:

- **MONITOR > Rogues > Friendly APs** to view rogue access points that are classified as Friendly.

  See Friendly Rogue APs for more information.
- **MONITOR > Rogues > Malicious APs** to view rogue access points that are classified as Malicious.

  See Malicious Rogue APs for more information.
- **MONITOR > Rogues > Custom APs** to view rogue access points that are classified as Custom.

  See Custom Rogue APs for more information.
- **MONITOR > Rogues > Unclassified APs** to view rogue access points that are unclassified.

  See Unclassified Rogue APs for more information.
- **MONITOR > Rogues > Rogue Clients** to view information about rogue clients that are detected.

  See Rogue Clients for more information.
- **MONITOR > Rogues > Adhoc Rogues** to view information about ad-hoc rogue clients that are detected.

  See Adhoc Rogues for more information.
- **MONITOR > Rogues > Rogue AP ignore-lists** to view the MAC addresses of access points that are configured to be ignored.

  See Rogue AP Ignore-list for more information.

Filtering AP Results by MAC Address

The rogue AP search results can be filtered by AP MAC address. This filter is available on all the **Monitor > Rogue** pages.

Step 1 Click **Change Filter**.

Step 2 Check the **MAC Address** check box.

Step 3 Enter the AP MAC address in the box.

Step 4 Click **Apply.**

Friendly Rogue APs

Choose **MONITOR > Rogues > Friendly APs** to navigate to the Friendly Rogue APs page.

This page displays rogue access points that are classified as Friendly.

Table 2-40 Friendly Rogue Access Point Parameters

Parameter	Description
MAC Address	MAC address of the rogue access point.
SSID	SSID that is broadcast by the rogue access point radio.
Channel	Channel number of the access point that has detected this friendly rogue access point.
# Detecting Radios	Number of Cisco Radios that detect the rogue access point radio.
Number of Clients	Number of clients associated with the rogue access point.
Status	Automatic and configurable state of this radio relative to the network or controller. The status of rogue access point radios is one of the following: • Internal—The unknown access point is inside the network and poses no threat to WLAN security. For example, the access points in your lab network is an internal rogue access point. • External—The unknown access point is outside the network and poses no threat to WLAN security. For example, the access points belonging to a neighboring coffee shop are external rogue access points. • Alert—The unknown access point is not in the neighbor list or in the user-configured friendly MAC list.

This page reports rogue access points until the “Expiration Timeout for Rogue AP Entries” (set on the Friendly Rogues page) expires.

The MAC address links in on this page take you to the respective Rogue AP Detail page when selected.

To remove rogue access points from the list, select the check boxes that correspond to the access point and click **Remove Selected**.

To remove all access points, select the check box in the table header row and access points are automatically selected. Click **Remove Selected**.

Malicious Rogue APs

Choose **MONITOR > Rogues > Malicious APs** to navigate to the Malicious Rogue APs page.

This page displays the rogue access points that are classified as Malicious. This page reports rogue access points until the "Expiration Timeout for Rogue AP Entries" (set on the Friendly Rogues page) expires.

The MAC address links in the rogue access point radios table take you to the respective Rogue AP Detail page when selected.

To remove a rogue access point from the list, click the blue arrow adjacent the desired rogue access point and choose **Remove**.

Table 2-41 Malicious Rogue Access Point Parameters

Parameter	Description
MAC Address	MAC address of the rogue access point.
SSID	SSID being broadcast by the rogue access point radio.
Channel	Channel number of the access point that has detected this rogue access point.
# Detecting Radios	Number of Cisco Radios that detect the rogue access point radio.
Number of Clients	Number of clients associated with the rogue access point.
Status	Automatic and configurable state of the radio relative to the network or controller. The status of rogue access point radios is one of the following: • Alert—The unknown access point is not in the neighbor list or in the user-configured friendly MAC list. • Threat—The unknown access point is found to be on the network and poses a threat to WLAN security. • Contained—The unknown access point is contained. • Containment Pending—The unknown access point is marked "Contained," but the action is delayed due to unavailable resources.

To remove rogue access points from the list, select the check boxes that correspond to the access point and click **Remove**.

To move the Malicious rogue APs that are being contained or were contained back to Alert state, click **Move to Alert** button on the respective pages.

To remove all access points, select the check box in the table header row. All access points are automatically selected. Click **Remove**.

Custom Rogue APs

Choose **MONITOR > Rogues > Custom APs** to navigate to the Custom Rogue APs page.

This page displays rogue access points that are classified as Custom.

Table 2-42 Custom Rogue Access Point Parameters

Parameter	Description
MAC Address	MAC address of the rogue access point.
SSID	SSID that is broadcast by the rogue access point radio.
Channel	Channel number of the access point that has detected this friendly rogue access point.
# Detecting Radios	Number of Cisco Radios that detect the rogue access point radio.
Number of Clients	Number of clients associated with the rogue access point.
Status	Automatic and configurable state of this radio relative to the network or controller. The status of rogue access point radios is one of the following: • Internal—The unknown access point is inside the network and poses no threat to WLAN security. For example, the access points in your lab network is an internal rogue access point. • External—The unknown access point is outside the network and poses no threat to WLAN security. For example, the access points belonging to a neighboring coffee shop are external rogue access points. • Alert—The unknown access point is not in the neighbor list or in the user-configured friendly MAC list.

This page reports rogue access points until the Expiration Timeout for Rogue AP Entries (set on the Friendly Rogues page) expires.

The MAC address links in on this page take you to the respective Rogue AP Detail page when selected.

To remove rogue access points from the list, select the check boxes that correspond to the access point and click **Remove**.

To remove all access points, select the check box in the table header row and access points are automatically selected. Click **Remove**.

Unclassified Rogue APs

Choose **MONITOR > Rogues > Unclassified APs** or **MONITOR > Summary** and click **Active Rogue APs** under the Rogue Summary section to navigate to the Unclassified Rogue APs page.

This page reports rogue access points until the expiration timeout for rogue AP entries (set on the Friendly Roguespage) expires. The MAC address links in the rogue access point radios table take you to the respective Rogue AP Detail page when selected.

To remove a rogue access point from the list, click the blue arrow adjacent the desired rogue access point and choose **Remove**.

This page displays rogue access points that did not match the Malicious or Friendly rules.

Table 2-43 Rogue Access Point Radio Parameters

Parameter	Description
MAC Address	MAC address of the rogue access point.
SSID	SSID being broadcast by the rogue access point radio.

Table 2-43 Rogue Access Point Radio Parameters

Parameter	Description
Channel	Channel number of the access point that has detected this unclassified rogue access point.
# Detecting Radios	Number of Cisco Radios that detect the rogue access point radio.
Number of Clients	Number of clients associated with the rogue access point.
Status	Automatic and configurable state of this radio relative to the network or controller. The status of rogue access point radios is one of the following: • Pending—On first detection, the unknown access point is put in the "Pending" state for 3 minutes. During this time, the managed access points determine if the unknown access point is a neighbor access point. • Alert—The unknown access point is not in the neighbor list or in the user-configured friendly MAC list. • Contained—The unknown access point is contained. • Containment Pending—The unknown access point is marked "Contained," but the action is delayed due to unavailable resources.

To remove rogue access points from the list, select the check boxes that correspond to the access point and click **Remove**.

To move the Malicious rogue APs that are being contained or were contained back to Alert state, click **Move to Alert** button on the respective pages.

To remove all access points, select the check box in the table header row. All access points are automatically selected. Click **Remove**.

Rogue AP Detail

Choose **MONITOR > Summary**, click **Detail** in the Active Rogue APs row of the Rogue Summary section, and then click the MAC address of the AP to navigate to the Rogue AP Detail page.

This page displays the access point details of the unauthorized or unknown radio. This table describes the new rule parameters.

Rogue Access Point Radio Details

Table 2-44 Rogue Access Point Radio Details

Parameter	Description
MAC Address	MAC address of the rogue access point.
Type	Rogue access point type: • AP—Infrastructure access point • Ad Hoc—Client-to-Client
Is Rogue on Wired Network?	Yes or No. Unknown if WEP is enabled, as shown below on this page.

Table 2-44 Rogue Access Point Radio Details

Parameter	Description
First Time Reported On	Date and time that the radio was first scanned by the controller.
Last Time Reported On	Date and time that the radio was last scanned by the controller.
Classification Change By	Classification of the rogue access point either manually, by default, or by rogue rule.
Class Type	Class of this radio as follows: • Friendly—An unknown access point that matches the user-defined friendly rules or an existing known and acknowledged rogue access point. Friendly access points cannot be contained. • Malicious—An unknown access point that matches the user-defined malicious rules or is moved manually by the user from the "Friendly" or "Unclassified" classification type. **Note** Once an access point is classified as "Malicious," you cannot apply rules to it in the future, and it cannot be moved to another classification type. If you want to move a malicious access point to the "Unclassified" classification type, you must delete the access point and allow the controller to reclassify it. • Unclassified—An unknown access point that does not match the user-defined friendly or malicious rules. An unclassified access point can be contained. It can also be moved to the "Friendly" or "Malicious" classification type automatically in accordance with user-defined rules or manually by the user. • Custom—An unknown access point that matches the user-defined classification type.
Manually Contained	Whether the rogue is manually contained or automatically contained.
State	Status of this radio as follows: • Alert • Internal • External • Contain • Pending

Table 2-44 Rogue Access Point Radio Details

Parameter	Description
Update Status[1]	Configurable state of this rogue access point in the controller. You may set the status to one of the following: • Internal—The controller trusts this rogue access point. This option is available if the Class Type is set to Friendly. • External—The controller acknowledges the presence of this rogue access point. This option is available if the Class Type is set to Friendly. • Contain—The controller contains the offending device so that its signals no longer interfere with authorized clients. This option is available if the Class Type is set to Malicious or Unclassified. • Alert—The controller forwards an immediate alert to the system administrator for further action. This option is available if the Class Type is set to Malicious or Unclassified.
Maximum number of APs to contain this rogue	Maximum number of access points used to contain this rogue (1, 2, 3, or 4).

1. Do not attempt to contain rogue access points operated by other establishments, such as the cafe hotspot across the street.

APs that Detected this Rogue

Table 2-45 APs that Detected this Rogue

Parameter	Description
Base Radio MAC	MAC address of the Cisco access point that identified the rogue access point radio.
AP Name	Name of the Cisco access point that identified the rogue access point radio.
SSID	SSID being broadcast by the rogue access point radio.
Channel	Channel the rogue access point is broadcasting on.
Channel Width (Mhz)	Channel bandwidth: 20 MHz or 40 MHz.
Radio Type	Protocol of the rogue access point that is either 802.11a, 802.11b, 802.11g, or 802.11n.
WEP	Whether WEP is enabled or disabled.
WPA	Type of security protocol is Enabled or Disabled.
Pre-Amble	Preamble type of the AP that detected this rogue.

Table 2-45 APs that Detected this Rogue

Parameter	Description
RSSI	Receive signal strength indicator (RSSI) of rogue access point radio at the access point. If RSSI indicates –80 dBm or lower, the rogue access point is far away or transmitting at a low signal strength. If RSSI indicates –60 dBm or higher, the rogue access point is close and/or transmitting at a high signal strength.
SNR	Signal to noise ratio (SNR) of rogue access point radio at the access point.
Containment Type	Contained if the rogue access point clients have been contained at Level 1 through Level 4 under Update Status Maximum Number; otherwise this field is blank.
Containment Channel	Current channel or channels if the rogue access point clients have been contained at Level 1 through Level 4 under Update Status; otherwise this field is blank.

Clients Associated with this Rogue AP

Table 2-46 Clients Associated with this Rogue AP

Parameter	Description
MAC Address	MAC address of the rogue client.
Last Time Heard	Last time the Cisco access point detected the rogue access point client.

Click **Apply** to send data to the controller, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Rogue Clients

Choose **MONITOR > Rogues > Rogue Clients** or **MONITOR > Summary** and click **Detail** in the Active Rogue Clients row of the Rogue Summary section to view the Rogue Clients page. This page displays information about rogue clients that are detected.

Table 2-47 Rogue Client Parameters

Parameters	Description
MAC Address	MAC address of the rogue client.
AP MAC Address	MAC address of the Cisco access point.
SSID	Service Set Identifier being broadcast by the rogue client.

Table 2-47 Rogue Client Parameters

Parameters	Description
# Detecting Radios	Number of Cisco radios detecting the rogue client.
Last Seen On	Last time that the Cisco access point detected the rogue access point client.
Status	Configurable state of this radio relative to the network or controller: • Contain—The controller contains the offending device so that its signals no longer interfere with authorized clients. • Alert—The controller forwards an immediate alert to the system administrator for further action.
Wired	Whether the client is on a wired network or not.

Rogue Client Details

Choose **MONITOR > Rogues > Rogue Clients** and then click the MAC address link to navigate to the Rogue Client Details page. This page displays details of unauthorized clients.

Rogue Client Details

Table 2-48 Rogue Client Detail Parameters

Parameter	Description
MAC Address	MAC address of the rogue access point.
APs MAC Address	MAC address of the Cisco access point that identified the rogue access point radio.
Radio Type	
SSID	SSID being broadcast by the rogue access point radio.
IP Address	IPv4 or IPv6 address of the rogue client or Unknown.
First Time Reported On	Date and time that the radio was first scanned by the controller.
Last Time Reported On	Date and time that the radio was last scanned by the controller.
State	Status of this radio is as follows: • Contain • Alert
Update Status[1]	Configurable state of this rogue access point in the controller. You may set the status to one of the following: • Contain—The controller contains the offending device so that its signals no longer interfere with authorized clients. • Alert—The controller forwards an immediate alert to the system administrator for further action.

1. Do not attempt to contain rogue access points operated by other establishments, such as the cafe hotspot across the street!

APs that Detected this Rogue Client

Table 2-49 APs Detected Rogue Clients Parameters

Parameter	Description
Base Radio MAC	MAC of the access point.
AP Name	Access points that identified the rogue access point radio.
Channel	Channel that the access point is broadcasting on.
Radio Type	Protocol of the rogue access point is either 802.11a, 802.11b, 802.11g, 802.11n, or Unknown.
RSSI	Receive signal strength indicator (RSSI) of access point radio at the access point. –80 dBm or lower, the rogue access point is far away or transmitting at a low signal strength. –60 dBm or higher, the rogue access point is close and/or transmitting at a high signal strength).
SNR	Signal to noise ratio (SNR) of the access point.

Click **Apply** to send data to the controller, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Click **Ping** to send a ping to a network element.

Adhoc Rogues

Choose **MONITOR > Rogues > Adhoc Rogues** or **MONITOR > Summary** and click **Detail** in the Adhoc Rogues row of the Rogue Summary section to navigate to the Adhoc Rogues page. You can see details of friendly, malicious, custom, and unclassified ad-hoc rogues in separate pages.

Table 2-50 Adhoc Rogues Parameters

Parameters	Description
MAC Address	MAC address of the rogue client.
BSSID	MAC address of the Cisco access point.
SSID	SSID that is broadcast by the rogue client.

Table 2-50 Adhoc Rogues Parameters

Parameters	Description
# Detecting Radios	Number of Cisco Radios that detect the rogue client.
Status	Status of this radio as follows: • Contain—The controller contains the offending device so that its signals no longer interfere with authorized clients. • Alert—The controller forwards an immediate alert to the system administrator for further action. • Internal—The controller trusts this rogue access point. • External—The controller acknowledges the presence of this rogue access point.

Adhoc Rogue Details

Choose **MONITOR > Rogues > Adhoc Rogues** and click the MAC address link in the ad-hoc rogue table to navigate to the Adhoc Rogues Details page.

This page displays details about ad-hoc rogue access points.

Adhoc Rogues

Table 2-51 Adhoc Rogues Details Parameters

Parameters	Description
MAC Address	MAC address of the ad-hoc rogue.
BSSID	BSSID of the ad-hoc rogue.
First Time Reported On	Date and time that the rogue was first scanned by the controller.
Last Time Reported On	Date and time that the rogue was last scanned by the controller.
Classification Change By	Classification of the rogue access point either manually, by default, or by rogue rule.
Classified by AP	MAC address of the access point that classified the rogue access point.
Classified RSSI	RSSI of the rogue access point.
Rule Name	Name of the custom rogue rule.
Severity Score	Custom classification severity score for the rogue rule. The range is from 1 to 100.
State Change By	Cause of the state change of the rogue access point.

Table 2-51 Adhoc Rogues Details Parameters

Parameters	Description
Class Type	Classification type of the rogue access point. It can be one of the following: • Friendly—An unknown access point that matches the user-defined friendly rules or an existing known and acknowledged rogue access point. Friendly access points cannot be contained. • Malicious—An unknown access point that matches the user-defined malicious rules or is moved manually by the user from the "Friendly" or "Unclassified" classification type. **Note** Once an access point is classified as "Malicious," you cannot apply rules to it in the future, and it cannot be moved to another classification type. If you want to move a malicious access point to the "Unclassified" classification type, you must delete the access point and allow the controller to reclassify it. • Unclassified—An unknown access point that does not match the user-defined friendly or malicious rules. An unclassified access point can be contained. It can also be moved to the "Friendly" or "Malicious" classification type automatically in accordance with user-defined rules or manually by the user. • Custom—An unknown access point that matches the user-defined classification type.
State	Current state of this rogue access point in the controller. It can be one of the following: • Internal—The controller trusts this rogue access point. This option is available if the Class Type is set to Friendly. • External—The controller acknowledges the presence of this rogue access point. This option is available if the Class Type is set to Friendly. • Contain—The controller contains the offending device so that its signals no longer interfere with authorized clients. This option is available if the Class Type is set to Malicious or Unclassified. • Alert—The controller forwards an immediate alert to the system administrator for further action. This option is available if the Class Type is set to Malicious or Unclassified.

Table 2-51 Adhoc Rogues Details Parameters

Parameters	Description
Update Status[1]	Configurable state of this rogue access point in the controller. You may set the status to one of the following: • Contain—The controller contains the offending device so that its signals no longer interfere with authorized clients. • Alert—The controller forwards an immediate alert to the system administrator for further action. • Internal—The controller trusts this rogue access point. • External—The controller acknowledges the presence of this rogue access point.
Maximum number of APs to contain this rogue	Maximum number of access points used to contain this rogue (1, 2, 3, or 4).

1. Do not attempt to contain rogue access points operated by other establishments, such as the cafe hotspot across the street!

APs that Detected this Rogue

Table 2-52 AP Detected Rogue Parameters

Parameter	Description
Base Radio MAC	MAC of the access point.
AP Name	Access points that identified the access point radio.
SSID	SSID of the access point.
Channel	Channel on which the rogue access point is broadcasting.
Radio Type	Protocol of the rogue access point that is either 802.11a, 802.11b, 802.11g, 802.11n, or Unknown.
WEP	Whether WEP is enabled on the access point.
WPA	Whether WPA is enabled on the access point.
Pre-Amble	Preamble type of either Long or Short.
RSSI	RSSI of the access point.
SNR	Signal to noise ratio (SNR) of the access point at the Cisco access point.
Containment Type	Type of containment.
Containment Channels	Channels on which the access point contained the ad-hoc rogue.

Click **Apply** to send data to the controller, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Rogue AP Ignore-list

Choose **MONITOR > Rogues > Rogue AP ignore-list** to navigate to the **Rogue AP Ignore-list** page.

This page shows the MAC addresses of any access points that are configured to be ignored.

The rogue-ignore list contains a list of any autonomous access points that have been manually added to Prime Infrastructure (PI) maps by PI users. The controller regards these autonomous access points as rogues even though Prime Infrastructure is managing them. The rogue-ignore list allows the controller to ignore these access points. The list is updated as follows:

- When the controller receives a rogue report, it checks to see if the unknown access point is in the rogue-ignore access point list.
- If the unknown access point is in the rogue-ignore list, the controller ignores this access point and continues to process other rogue access points.
- If the unknown access point is not in the rogue-ignore list, the controller sends a trap to PI . If PI finds this access point in its autonomous access point list, PI sends a command to the controller to add this access point to the rogue-ignore list. This access point is then ignored in future rogue reports.
- If you remove an autonomous access point from the PI, the PI sends a command to the controller to remove this access point from the rogue-ignore list.

Redundancy

Choose **MONITOR > Redundancy** to view information about redundancy. The available options are as follows:

- To view redundancy statistics, choose **MONITOR > Redundancy > Statistics**.

  See Redundancy Statistics more information.
- To view redundancy peer statistics, choose **MONITOR > Redundancy > Peer Statistics**.

  See
- To view the redundancy summary, choose **MONITOR > Redundancy > Summary**.

  See Redundancy Summary more information.

Redundancy Statistics

Choose **MONITOR > Redundancy > Statistics** to navigate to the Redundancy Statistics page.

This page displays information about the redundancy statistics.

Note You can view the redundancy statistics only if the SSO mode is enabled.

Table 2-53 Redundancy Statistics

Parameter	Description
Category	Drop down box from which you can select one of the following category: • All • Infra • Transport • Keepalive • GW-Reachability • Config-Sync • None
RF Client Brief	Displays the RF Clients list.
Sanity Counters	
Sanity Messages successfully sent	Displays the number of Sanity messages i.e. health check messages sent from this box.
Sanity Messages failed to send	Displays the number of Sanity messages failed to send from the controller.
Sanity Messages received from peer	Displays the number of Sanity messages received from the Peer WLC.
Transport Counters	
Number of messages in the hold Queue	Displays information about number of IPC messages in queue.
Application message Max Size	Displays information about number of IPC messages in queue.
IPC message Max Size	Displays maximum supported MTU size IPC messages.
Time to hold IPC messages	Displays maximum time to hold the IPC messages if the IPC buffer is not full.
IPC sequence number in the TX side	Displays IPC sequence number in the transmitter window.
IPC sequence number in the RX side	Displays IPC sequence number in the receiver window.
IPC sequence number mismatches (Low)	Displays low watermark of IPC sequence number mismatches.
IPC sequence number mismatches (high)	Displays high watermark of IPC sequence number mismatches.
Keepalive Counters	
Keep Alive Request Received	Displays the number of Keep Alive request received from the peer through RP.
Keep Alive Responses Received	Displays the number of Keep Alive response received from the peer through RP.
Keep Alive Request Sent	Displays the number of Keep Alive Requests sent to peer.

Table 2-53 Redundancy Statistics

Parameter	Description
Keep Alive Response Sent	Displays the number of Keep Alive Responses sent from the controller.
Keep Alive Requests failed to send	Displays the number of Keep Alive Requests failed to send from the controller.
Keep Alive Responses to failed to send	Displays the number of Keep Alive Responses failed to send from the controller.
Number of times two Keep alives are lost consecutively	Displays the number of times 2 keepalives are lost consecutively. i.e twice did not get the response for keep alive requests.
Network Latencies (RTT) for the Peer Reachability in microsec	
Peer Reachability Latency	Displays the latency between peers through RMI.
Gx Reachability	
Gw Pings Succesfully sent	Displays the number of Pings successfully sent to Gateway from the controller.
Gw Pings Failed to send	Displays the number of Pings failed to send to Gateway from the controller.
Gw Responses Received	Displays the number of Pings successfully received from the Gateway to the controller.
Current consecutive Gw Responses Lost	Displays the number of consecutive GW responses lost i.e number of consecutive responses not received.
High Water Mark of Gw Responses Lost	Displays the highest consecutive GW responses lost to the controller.
Network Latencies (RTT) for the Management Gateway Reachability in microsec	
Gateway Reachability Latency	Displays the latency between the controller and the GW.
Ping Request and Response	
Ping Requests sent to Peer	Displays the number of ping requests sent to peer through RMI.
Ping Response received from Peer	Displays the number of ping responses received from the peer through RMI.
Config Sync Counter	
Usmdb Functions sent for Sync	Displays the total number of Usmdb functions sent for Sync to Standby
Failed sync for Usmdb Sync	Displays the total number of Usmdb functions failed to send for Sync to Standby.
UsmDbs which failed to sync from Active to Standby	
Index	Displays the index of UsmDb failed to sync.
Failed UsmDb	Displays the information about the UsmDb that is failed to sync to standby.
Port Information	

Table 2-53 Redundancy Statistics

Parameter	Description
Local Physical Ports	Indicate the ports that are operationally up in the controller.
Peer Physical Ports	Indicate the ports that are operationally up in the peer controller.

Peer Statistics

Choose **MONITOR > Redundancy > Peer Statistics** to navigate to the Peer Statistics page.

The CPU and memory statistics of all the threads of the standby WLC are synchronized with the active controller every 10 seconds. This information is displayed when you query for the peer statistics on the active WLC.

This page displays the following information:

- Peer-System statistics
- Peer-Process CPU statistics
- Peer-Process Memory statistics

Redundancy Summary

Choose **MONITOR > Redundancy > Summary** to navigate to the Redundancy Summary page.

This page displays information about the Redundancy Facilitator states on the active and peer unit in the redundancy mode and the switch of activity (swact).

Table 2-54 Redundancy Facilitator Summary

Parameter	Description
Local State	Current state of the Redundancy Facilitator of the controller. It can be Active, Standby HOT, or Standby COLD.
Peer State	Current state of the Redundancy Facilitator of the peer controller. It can be Active, or Standby HOT, or Standby COLD.
Unit	Type of controller that can be primary or secondary.
Unit ID	Unique ID of the redundant unit. It can be the MAC address of the controller.
Redundancy State	Redundancy mode operational on the controller. The redundancy modes are as follows: • 0—No redundancy • SSO—Hot Standby Mode • RPR—Cold Standby Mode
Maintenance Mode	Maintenance mode that can be enabled or disabled. Indicates if the redundant units can communicate synch messages with each other. If the controllers cannot reach each other through the redundant port or through the Redundant Management Interface, the standby controller goes into the maintenance mode.

Table 2-54 Redundancy Facilitator Summary (continued)

Parameter	Description
Maintenance Cause	Cause of the switchover to the maintenance mode.
Average Redundancy Peer Reachability Latency	Average delay to reach the peer controller in seconds.
Average Management Gateway Reachability Latency	Average delay to reach the management gateway in seconds.
BulkSync Status	Indicates whether the bulk sync is completed once the Standby boots up and moves to STANDBY HOT state. This can be: • In-Progress • Pending and • Complete

Redundancy Detail

Choose **MONITOR > Redundancy > Detail** to navigate to the Redundancy details page.

Table 2-55 Redundancy Detail Parameters

Parameter	Description
Redundancy Management	This is the IP address of Redundancy Management Interface of the controller.
Peer Redundancy Management	This is the IP address of the Redundancy Management Address of the Peer controller.
Redundancy port IP	This is the IP address of the Redundancy Port of the controller.
Peer Redundancy port IP	This is the IP address of the Redundancy Port of the Peer controller.
Peer Service Port IP	This is the IP address of the Service port of the Peer controller.
Switchover History Table	
Previous Active	Information about controller that was previously Active before Switchover. This will have the RMI IP of previous Active.
Current Active	Information about controller that was currently Active after Switchover. This will have the RMI IP of current Active.
Switchover Reason	Information about the switchover reason whether it is User initiated, GW not reachable or Active Failed.
Switchover Time	Information about when the switchover has happened.
Redundancy Timeout Values	
Keep Alive TimeOut	Information about the timeout the controller can wait for Keep Alive responses before considering keep alive is lost.
Peer Search TimeOut	Information about the timeout the controller can wait for peer search responses before considering peer is not reachable.
Network Routes Peer	

Table 2-55 Redundancy Detail Parameters (continued)

Parameter	Description
Number of Routes	Total number of Network Routes this controller holds.
IP Address	IP address of target network/IP address.
IP Netmask	IP network mask information of the routes of this controller.
Gateway IP Address	Information about the next hop gateway for this route.

Clients

Choose **MONITOR > Clients** or **MONITOR > Summary** and click **Detail** in the row that corresponds to Current Clients in the Client Summary section to navigate to the Clients page.

This page displays information about the clients associated with the access points.

Client List Filter

You can create a filter to display the client list by MAC address or a combination of access point name, WLAN profile name, status, radio type, workgroup bridge (WGB), or PMIP.

Note When you enable the MAC address filter, other filter options are disabled.

When you enable the AP name, WLAN profile name, status, radio type, or workgroup bridge (WGB) filter, the MAC address filter is disabled.

The current filter parameters are displayed in the Current Filter field.

Click **Change Filter** to display the Search Clients dialog box (see the following figure) and to create or change filter parameters. Click **Show All** to remove the filter and display the entire client list.

- MAC Address—MAC address that you enter as 6 two-digit hexadecimal numbers separated by colons (for example, 01:23:45:67:89:AB).
- IP Address—IP address of the client.
- AP Name—Access point name.
- User Name—Username associated with the client.
- WLAN Profile—WLAN profile name. You can select a WLAN profile by selecting one of the configured WLANs on your wireless network.
- WLAN SSID—SSID of the WLAN that the client is associated with.
- Status—One or more status types: Associated, Authenticated, Excluded, Idle.
- Radio Type—802.11a, 802.11b, 802.11g, 802.11an, 802.11bn, Mobile radio type.
- WGB—WGB wired clients that are associated with the access points.
- Apply—Filter settings.

Client Information Table

This table displays a list of all clients attached to the controller. Client information includes the following:

- Client MAC Addr—MAC address of the client.
- IP Address—IP address of the client.
- AP Name—Name of the access point.
- WLAN Profile—Name of the WLAN used by the client.
- WLAN SSID—SSID of the WLAN that the client is associated with.
- User Name—Username associated with the client.
- Protocol—Remote LAN clients that shows Ethernet as the protocol.
- Status—Status of the client connection.
- Auth—Authorization status.
- Port—Port number of the client's associated access point.
- Slot ID—Slot number of the interface that can be from 0 to 3 that the client is connected to.
- PMIPv6—Whether the client is a PMIP client.
- WGB—Workgroup bridge (WGB) status.

  A workgroup bridge is a mode that can be configured on an autonomous Cisco IOS access point to provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the WGB access point.
- Device Type—Type of client device.

Click the blue arrow adjacent the desired client and choose one of the following:

- Show Wired Clients—Shows details of any wired clients that are connected to a particular WGB on the WGB Wired Clients topic. (This option is available if the client is a WGB.)
- LinkTest—Tests the link to the client, reports the client MAC address, and reports the number of test packets sent and received, the local signal strength, and the local signal to noise ratio. The LinkTest does not work for IPsec links and may not work for some clients.
- Disable—Manually disables a client on the Adding Disabled Clients page.
- Remove—Dissociates the client.
- 802.11aTSM or 802.11b/gTSM—Displays Traffic Stream Metrics for these radios.

Click the MAC address of the desired client to display the Client Details page.

Client Details

Choose **MONITOR > Clients** and then click the client MAC address to navigate to the Client Details page.

This page displays the details of the client's session and the AVC statistics. Information is displayed for both the client and its associated access point.

You can view the top 10 applications used by the client in the AVC Statistics tab. Client statistics are only collected for the first 128 applications classified in 90 seconds.

Client Properties

Table 2-56 Client Properties Parameters

Parameter	Description
MAC Address	MAC address of the client.
IPv4 Address	List of IPv4 address of the clients.
IPv6 Address	List the IPv6 address of the clients.
Client Type	Regular, WGB, WGB client, or Unknown type.
Number of Wired Client(s)	Number of wired clients that are connected to this WGB if the client type is WGB.
User Name	Login client name from RADIUS or controller authentication.
Port Number	Controller port used for the client's associated access point.
Interface	User-defined name for this interface; for example, management, service-port, virtual.
VLAN ID	VLAN tag identifier, or 0 for no VLAN tag.
CCX Version	Cisco Client Extensions (CCX) version in use, if supported. If the client supports Cisco Client Extensions version 5, two additional button are displayed: • Send CCXV5 Request • Display See the Client Reporting page for more information about Cisco Client Extensions version 5 client reporting.
E2E Version	End-to-End version in use, if supported.
Mobility Role	Local when the client has not roamed from its original controller or when the client has roamed to another controller on the same subnet. Foreign when the client has roamed from its original controller to another controller on a different subnet. Anchor when the client has roamed back to its original controller after roaming to another controller on a different subnet.
Mobility Peer IP Address	N/A when the client is Local (has not roamed from its original subnet). Anchor IP address (the IP address of the original controller) when the client is Foreign (has roamed to another controller on a different subnet). Foreign IP address (the IP address of the original controller) when the client is Anchor (has roamed back to another controller on a different subnet).
Policy Manager State	DHCP_REQD when a DHCP server is required to complete the security policy. 8021X_REQD when 802.1X is the required policy. Other messages to be determined.
Management Frame Protection	Management frame protection (MFP) provides security for the unprotected and unencrypted 802.11 management messages passed between access points and clients. MFP provides both infrastructure and client support.

Table 2-56 Client Properties Parameters

Parameter	Description
UpTime (Sec)	Time in seconds since the client has been up.
Power Save Mode	Power save mode of the client.
Current TxRateSet	Current transmission rate.
Data RateSet	Data rate for the client.
KTS CAC Capability	KTS-based CAC capability of the client.
802.11u	Hotspot is a solution that enables 802.1X capable clients to interwork with external networks. This feature provides service availability information to clients and can help them to associate available networks.
802.11v BSS Transition	802.11v refers to the IEEE (Institute of Electrical and Electronics Engineers) 802.11 Wireless Network Management (Amendment 8). Stations that supports WNM (Wireless network management) can exchange information with each other (Access Points and wireless clients) in order to improve their performance.
Fastlane Client	Specifies whether the client has Fastlane QoS.

Security Information

Table 2-57 Security Information Parameters

Parameter	Description
Security Policy Completed	No (when the security policy checks have not been completed) or Yes (when the security policy checks have been completed).
Auth Key Mgmt	Type of Authenticated Key Management that can be one of the following: • 802.1X • CCKM • PSK • FT 802.1X • FT PSK • SUITEB-1X • SUITEB192-1X • 802.1X+CCKM • WPA gtk-randomize State
EAP Type	–
SNMP NAC State	Current state of the client: Quarantine, Access, or Invalid.
RADIUS NAC State	Current state of the client in the RADIUS NAC-enabled WLAN. When a client is associated to the controller on a RADIUS NAC-enabled WLAN, the controller forwards the request to the ISE server. The state of the client can be DHCP_REQD or POSTURE_REQD.
CTS Security Group Tag	Cisco TrustSec Security Group Tag information.

Table 2-57 Security Information Parameters

Parameter	Description
AAA Override ACL Name	Name of the AAA Override ACL. This ACL is in addition to the VLAN ACL that is applied to the VLAN on the Ethernet interface. If a client gets an AAA Override of the VLAN, the client is placed on the overridden VLAN and the ACL on the VLAN applies to the client. To support centralized access control through an AAA server, such as ISE or ACS, an ACL must be configured on the controller and the WLAN must be configured with the AAA override-enabled feature.
AAA Override ACL Applied Status	Status of the client that indicates if the client has been authenticated after the application of an AAA Override ACL.
AAA Override Flex ACL	Name of the IPv4 ACL that is the FlexConnect ACL for clients connected to FlexConnect access points.
AAA Override Flex ACL Applied Status	Status of the client that indicates if the client has been authenticated after the application of the AAA Override FlexConnect ACL.
Redirect URL	Redirect URL that the client should be directed to after authentication.
IPv4 ACL Name	Name of the IPv4 ACL.
IPv4 ACL Applied Status	Status of whether the IPv4 ACL was applied to the client's WLAN.
IPv6 ACL Name	Name of the IPv6 ACL.
IPv6 ACL Applied Status	Status of whether the IPv6 ACL was applied to the client's WLAN.
mDNS Profile Name	mDNS profile associated with the service that the client is using.
mDNS Service Advertisement Count	Count of the mDNS service advertisements that the client received for a requested service.
AAA Role Type	Role of the user.
Local Policy Applied	Policy applied to the client device.

Quality of Service Properties

Table 2-58 Quality of Service Parameters

Parameter	Description
WMM State	WMM state that you enable or disable. Wi-Fi Multimedia (WMM) is a QoS protocol and a subset of 802.11e standard. WMM technology identifies packets of voice, video, audio or other types of data and prioritizes their delivery based on traffic conditions. Videos transmitted over wireless networks suffer greatly if packets are delayed or dropped. So video data is given priority over other types of data on a network.
QoS Level	Quality of Service level that you set on the Editing QoS Profile page: • 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. VoIP clients should be set to Platinum, Gold or Silver, while low-bandwidth clients can be set to Bronze.
Diff Serv Code Point (DSCP)	Prioritization of packets by the 6 bits in the DSCP that you set on the Editing QoS Profile page.
802.1P Tag	VLAN tag (1-7) received from the client, defining the access priority. This tag maps to the QoS Level for client-to-network packets. You set this tag on the Editing QoS Profile page.
Average Data Rate	Operator-defined average data rate for non-UDP traffic that you set on the Editing QoS Profile page.
Average Real-Time Rate	Operator-defined average data rate for UDP traffic that you set on the Editing QoS Profile page.
Burst Data Rate	Operator-defined peak data rate for non-UDP traffic that you set on the Editing QoS Profile page.
Burst Real-Time Rate	Operator-defined peak data rate for UDP traffic that you set on the Editing QoS Profile page.

Client Statistics

Table 2-59 Client Statistics Parameters

Parameter	Description
Bytes Received	Number of bytes received by the controller from the client.
Bytes Sent	Number of bytes sent to the client from the controller.
Packets Received	Number of packets received by the controller from the client.
Packets Sent	Number of packets sent to the client from the controller.
Policy Errors	Number of policy errors for the client.
RSSI	Receive signal strength indicator of the client RF session.
SNR	Signal to Noise Ratio of the client.

Table 2-59 Client Statistics Parameters

Parameter	Description
Sample Time	Time that the client statistics snapshot was taken.
Excessive Retries	Number of excessive retries before the access point looks for another controller.
Retries	Number of retries before the access point finds a controller.
Success Count	Counter increments when a CTS is received in response to an RTS.
Fail Count	Modem failure count.
Tx Filtered	Number of filtered error frames.
Data Retries	Number of data retries by the client.
RTS Retries	Number of request-to-send retries by the client.
Duplicates	Number of duplicate packets received.
Decrypt Failed	Number of decrypt packets that failed.
Mic Errors	Number of packets that have MIC errors.
Mic Missing Frames	Number of packets that do not have MIC.
RA Packets Dropped	Number of router advertisement packets that are dropped.
Interim Updates Sent	Number of times the interim updates were sent.

Client Rate Limiting Statistics

Table 2-60 Client Rate Limiting Statistics Parameters

Parameter	Description
Data Bytes Received	Number of data bytes received by the controller from the client.
Data Rx Bytes Dropped	Number of Rx data bytes dropped by the controller from the client.
Data Rx Packets Dropped	Number of Rx packets dropped by the controller from the client.
Real-time Packets Received	Number of real-time packets received by the controller from the client.
Real-time Rx Packets Dropped	Number of Rx real-time packets dropped by the controller from the client.
Real-time Bytes Received	Number of real-time bytes received by the controller from the client.
Rx Data Bytes Dropped	Number of Rx data bytes dropped by the controller from the client.
Rx Real-time Bytes Dropped	Number of Rx real-time bytes dropped by the controller from the client.
Data Packets Sent	Number of packets sent to the client from the controller.
Data Bytes Sent	Number of data bytes sent to the client from the controller.
Real-time Bytes Sent	Number of real-time bytes sent to the client from the controller.
Tx Data Bytes Dropped	Number of Tx data bytes dropped by the controller from the client.
Tx Real-time Bytes Dropped	Number of Tx real-time bytes dropped by the controller from the client.
Data Packets Received	Number of data packets received by the controller from the client.

Table 2-60 Client Rate Limiting Statistics Parameters

Parameter	Description
Real-time Packets Sent	Number of real-time packets sent to the client from the controller.
Real-time Tx Packets Dropped	Number of Tx real-time packets dropped by the controller from the client.
Tx Data Packets Dropped	Number of Tx data packets dropped by the controller from the client.
Tx Real-time Bytes Dropped	Number of Tx real-time packets dropped by the controller from the client.

PMIP Properties

Table 2-61 PMIP Properties

Parameter	Description
Mobility Type	Type of PMIP mobility for the client. The type can be None or PMIPv6.
Network Access ID (NAI)	Network Access ID of the PMIP profile.
PMIP State	State state of the PMIP client. The available states are as follows: • Unknown—Indicates that the state of the client cannot be determined. • Activated—Indicates that the client is ready to establish a tunnel. • Tunneled—Indicates that a bidirectional tunnel is established.
Connected Interface	Connected interface of the controller.
Home Address	Address of the mobile node. The mobile node can use this address if it is attached to the access network that is in the scope of that Proxy Mobile IPv6 domain.

Table 2-61 PMIP Properties

Parameter	Description
Access Technology Type (ATT)	8-bit field that specifies the access technology through which the mobile node is connected to the access link on the Mobile Access Gateway (MAG). The values and the corresponding access technology are as follows: • 0—Reserved • 1—Logical Network Interface • 2—Point-to-Point Protocol • 3—Ethernet • 4—Wireless LAN • 5—WIMAX • 6—3GPP GSM EDGE Radio Access Network (3GPP GERAN) • 7—3GPP Universal Terrestrial Radio Access Network (3GPP UTRAN) • 8—3GPP ETRAN (3GPP Evolutions of the Transport in the UTRAN) • 9—3GPP2 eHRPD (3GPP2 Evolved High Rate Packet Data) • 10—3GPP2 HRPD (3GPP2 High Rate Packet Data) • 11—3GPP2 1xRTT • 12—3GPP2 UMB (3GPP2 Ultra Mobile Broadband)
Local Link Identifier	Local link identifier of the client.
LMA Name	Name of the LMA to which the client is connected.
Life Time	Duration of the PMIP client association.

AP Properties

Note The AP Properties table identifies the properties of the access point of the client and of the negotiated session of the client.

Table 2-62 AP Properties Parameters

Parameter	Description
AP Address	MAC address of the access point.
AP Name	Name of the access point.
AP Type	Access point's RF type.
AP radio Slot ID	Slot ID of the AP radio.
WLAN Profile	Name of the WLAN.
Status	Status of client from status code (see Status Code below).
Association ID	Client's access point association identification number.
802.11 Authentication	Authentication algorithm of client.

Table 2-62 AP Properties Parameters

Parameter	Description
Reason Code	Client reason code: • no reason code (0)—Normal operation. • unspecified reason (1)—The client is associated but no longer authorized. • previousAuthNotValid (2)—The client is associated but not authorized. • deauthenticationLeaving (3)—The access point went offline, deauthenticating the client. • disassociationDueToInactivity (4)—The client session timeout has been exceeded. • disassociationAPBusy (5)—The access point is busy (performing load balancing, for example). • class2FrameFromNonAuthStation (6)—The client attempted to transfer data before it was authenticated. • class2FrameFromNonAssStation (7)—The client attempted to transfer data before it was associated. • disassociationStaHasLeft (8)—The operating system moved the client to another access point using nonaggressive load balancing. • staReqAssociationWithoutAuth (9)—The client has not been authorized yet; the client has been attempting to associate with access point. • missingReasonCode (99)—The client was momentarily in an unknown state.
Status Code	Client status code: • idle (0)—Normal operation: no rejections of client association requests. • aaaPending (1)—The client is completing an AAA transaction. • authenticated (2)—802.11 authentication is completed. • associated (3)—802.11 association is completed. • powersave (4)—The client is in powersave mode. • disassociated (5)—802.11 disassociation is completed. • tobedeleted (6)—To be deleted after disassociation. • probing (7)—The client has not been associated or authorized yet. • disabled (8)—The client has automatically been disabled by the Operating System for an operator-defined time.
CF Pollable	Whether the client is able to respond to a CF-Poll with a data frame within a SIFS time. This attribute is not implemented if the STA is not able to respond to a CF-Poll with a data frame within a SIFS time.
CF Poll Request	Whether CFP is requested by the client.

Table 2-62 AP Properties Parameters

Parameter	Description
Short Preamble	Attribute, when true, that indicates that the short preamble option as defined in subclause 18.2.2.2 is implemented. This parameter must be disabled to optimize this controller for some clients, including SpectraLink NetLink Telephones.
PBCC	Attribute, when true, that indicates that the PBCC modulation option as defined in subclause 18.4.6.6 is implemented. The default value of this attribute is not implemented.
Channel Agility	Physical channel agility functionality that is or is not implemented.
Timeout	Client Session timeout (maximum amount of time before a client is forced to reauthenticate).
WEP State	WEP security state of the client.
Data Switching	Whether the client's data traffic is local or centrally switched. It shows up only for FlexConnect associated clients.

AVC Statistics

You can view the last 90 seconds and the cumulative statistics of the top 10 applications used by the client as a pie chart. Each application appears with the corresponding usage percentage. The applications are color coded for clarity. You can also view details of the applications such as packet count, byte count, and average packet size. Client statistics are only collected for the first 128 applications classified in 90 seconds. You can see upstream and downstream AVC statistics for the client.

This section describes the following command buttons:

- Click **Apply** to send data to the controller, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Click **Link Test** to use the built-in test circuitry to test the link between the client and the controller, reports the client MAC address, and reports the number of test packets sent and received, the local signal strength, and the local signal to noise ratio. LinkTest does not work for IPsec links and may not work for some clients.
- Click **Remove** to disconnect the client. If the client supports Cisco Client Extensions version 5, two additional buttons are displayed:
  - Click **Send CCXV5 Request** send the report request to the client.
  - Click **Display** to open the Client Reporting page.

WGB Wired Clients

The WGB Wired Clients page displays information about the WGB wired clients that are associated with the access points.

Note The WGB supports a maximum of 20 wired clients. If you have more than 20 wired clients, use a bridge or another device.

Client Information Table

This table displays a list of all clients attached to the controller. Client information includes the following:

- WGB MAC address
- MAC address of the client
- Name of the access point to which client is attached
- Name of WLAN used by the client
- Type of client (802.11a, 802.11b, 802.11g, or 802.11n)
- Status of the client connection
- Authorization status
- Port number of the client's associated access point

Click the blue arrow adjacent the desired client and choose one of the following:

- LinkTest—Indicates that the Link Test is not supported for WGB-wired clients.
- Disable—Manually disables a client on the Adding Disabled Clients page.
- Remove—Dissociates the client.
- 802.11aTSM or 802.11b/gTSM—Displays Traffic Stream Metrics for these radios.

Click the MAC address of the desired client to display the Client Details page.

Traffic Stream Metrics Collection

Choose **MONITOR > Clients** and click **802aTSM** or **802b/gTSM** to navigate to the Traffic Stream Metrics Collection page.

Traffic stream metrics (TSM) involves collecting of uplink statistics and downlink statistics between an access point and a CCX v4 client and then propagating these statistics periodically back to the controller. If the client is not CCXv4 compliant, then only the downlink statistics are captured. You configure traffic stream metrics collection on a per-interface band basis (such as all 802.11a/n radios). The controller saves this option in flash memory so that it persists across reboots. Once an access point receives this message, it enables the traffic metrics collection on the specified interface type.

Every 5 seconds, the access point gets a measurement report for both the uplink (client side) and downlink (local side) measurements. The aggregation of 5-second reports and preparation of 90-second reports are done at the access point. Every 90 seconds, the access point prepares an IAPP data packet and sends it to the controller for further processing. The controller stores the data in its structures and then provides "usmdB" access ChooseAPIs to the CLI module and the PI for displaying it on the UI.

Four variables are affected by the WLAN that can affect audio quality:

- Packet latency
- Packet jitter
- Packet loss
- Roaming time

You can isolate the problem of bad voice quality by studying these variables. The traffic stream metrics feature addresses the voice quality issue by providing statistics for each of these four variables.

Client Reporting

The Client Reporting page displays details about the client and wireless network adapter.

Table 2-63 Client Reporting Parameters

Parameter	Description
Client Profile	Displays all the available configuration profiles as well as the current profile in use on the wireless network adaptor. Click a profile name to display the Profile Details page.
Operating Parameters	Displays various operating settings that the client is currently using.
Manufacturer's Information	Displays all the static manufacturer-specific data about the client and wireless network adapter.
Client Capability	Displays the range of capabilities that are available on the wireless network adapter.

Note This group displays the available capabilities, not current settings.

Profile Details

The Profile Details page displays the details about the selected profile on the wireless network adapter.

Sleeping Clients

Choose **MONITOR > Sleeping Clients** to navigate to the Sleeping Clients page. This page displays details about the sleeping clients that are managed by the WLANs configured in the controller.

Table 2-64 Sleeping Clients Parameters

Parameter	Description
Client MAC	MAC address of the client.
WLAN SSID	SSID of the WLAN that the client is associated with.
User Name	Username associated with the client.
Remaining Time	Time, in hours and minutes, after the idle timeout of the sleeping client.

Multicast Groups

Choose **MONITOR > Multicast** to navigate to the Multicast page.

This page displays the details of the Layer 3 and Layer 2 multicast groups and their corresponding multicast group IDs (MGIDs).

Click the link for a specific MGID to see a list of all the clients joined to the multicast group in that particular MGID.

Layer 3 MGID Mapping

Table 2-65 Layer 3 MGID Parameters

Parameter	Description
Group address	Layer 3 MGID group address.
VLAN	Layer 3 MGID group VLAN.
MGID	Layer 3 MGID.
IGMP/MLD	Internet Group Management Protocol (IGMP) snooping that is used to limit the flooding of multicast traffic for IPv4. For IPv6, Multicast Listener Discovery (MLD) snooping is used.

Layer 2 MGID Mapping

Table 2-66 Layer 2 MGID Parameters

Parameter	Description
Interface name	Layer 2 MGID interface name.
VLAN ID	Layer 2 MGID VLAN ID.
MGID	Layer 2 multicast group ID.

Applications

Applications > WLAN

Choose **MONITOR > Applications > WLAN** to navigate to the **WLANs** page.

This page displays details of the WLANs that have Application Visibility and Control (AVC) profiles configured on them. Click the WLAN ID to navigate to the **WLANs > Application Statistics** page. Only WLANS on local mode access points or centrally switched on a FlexConnect access point are capable of having applications recognized by NBAR.

You can view the last 90 seconds and the cumulative statistics of the top 10 applications as a pie chart. Each application appears with the corresponding usage percentage. The applications are color coded for clarity. You can also view details of the applications such as packet count, byte count, and average packet size.

Applications > FlexConnect Groups

Choose **MONITOR > Applications > FlexConnect Groups** to navigate to the **FlexConnect Groups** page.

This page displays details of the FlexConnect groups that have Application Visibility and Control (AVC) profiles configured on them.

Lync

This section contains the following topics:

Active Calls

Choose **MONITOR > Lync > Active Calls** to navigate to Lync Active Calls page. This page shows the following call details:

- ID
- Call Type
- Caller User ID
- Caller IP Address (IPv4/IPv6)
- Caller MAC Address
- Caller AP Name
- Callee User ID
- Callee IP Address (IPv4/IPv6)
- Callee MAC Address
- Callee AP Name

History Calls

Choose **MONITOR > Lync > History Calls** to navigate to Lync History Calls page. This page shows the following call details:

- ID
- Call Type
- Caller IP
- Caller MAC Address
- Callee IP
- Callee MAC Address
- Status
- Duration

- MOS
- Jitter

Local Profiling

This page shows the following information:

- Device Stats
- Device Type and Count
- Manufacturer Stats
- Manufacturer Type and Count

Note This page displays only top 10 client counts.