CHAPTER 5

Monitoring Devices

Information About Monitoring

This chapter describes how to use Cisco NCS to monitor Cisco WLAN Solution device configurations. This chapter contains the following sections:

Monitoring Controllers

Choose **Monitor > Controllers** to access the controller list page. Click a controller IP address to view its details.

This section contains the following topics:

- Monitoring Controllers Mobility, page 5-23
- Monitoring Controller 802.11a/n, page 5-24
- Monitoring Controllers 802.11b/g/n, page 5-28

Searching Controllers

Use the NCS Search feature to find specific controllers or to create and save custom searches.

For a controller search, you can search using the following parameters:

Table 5-1 Search Controllers

Parameter	Description
Search for controller by	Choose All Controllers, IP Address, Controller Name, or Network. **Note** Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Enter Controller IP Address	This field only appears if you select IP Address from the Search for controller by field.
Enter Controller Name	This field only appears if you select Controller Name from the Search for controller by field.
Select a Network	
Audit Status	Choose one of the following from the drop-down list: – All Status – Mismatch—Config differences were found between NCS and controller during the last audit. – Identical—No config differences were found during the last audit. – Not Available—Audit status is unavailable.

See one of the following topics for additional information:

- Using the Search Feature, page 2-33
- Quick Search, page 2-33
- Advanced Search, page 2-34
- Saved Searches, page 2-46

Viewing List of Controllers

Choose **Monitor > Controllers** or perform a controller search to access the controller list page.

Note See the "Advanced Search" section on page 2-34 for more information on performing an advanced search.

The data area of this page contains a table with the following columns:

Table 5-2 Controller List Details

Parameter	Description
IP Address	Local network IP address of the controller management interface. Click an IP address in the list to display the controller details.
Controller Name	Name of the Controller.
Location	The geographical location (such as a campus or building).
Mobility Group Name	Name of the controller mobility or WPS group.
Reachability Status	Reachable or Unreachable. Click the title to toggle from ascending to descending order.

Click the title to toggle from ascending to descending order. To add, remove, or reorder columns in the table, click the **Edit View** link to go to the Edit View page.

Configuring the Controller List Display

The **Edit View** page allows you to add, remove, or reorder columns in the Controllers table.

To edit the available columns in the controllers table, follow these steps:

Step 1 Choose **Monitor > Controllers**.

Step 2 Click the **Edit View** link.

Step 3 To add an additional column to the controllers table, click to highlight the column heading in the left list. Click **Show** to move the heading to the right list. All items in the right list are displayed in the controllers table.

Step 4 To remove a column from the controllers table, click to highlight the list heading in the right list. Click **Hide** to move the heading to the left list. All items in the left list are not displayed in the controllers table.

Step 5 Use the **Up/Down** buttons to specify the order in which the information appears in the table. Highlight the desired list heading and click **Up** or **Down** to move it higher or lower in the current list.

Step 6 Click **Reset** to restore the default view.

Step 7 Click **Submit** to confirm the changes.

Monitoring System Parameters

This section provides the detailed information regarding monitoring controller system parameters and contains the following topics:

- Monitoring System Summary, page 5-4
- Monitoring Spanning Tree Protocol, page 5-5
- Monitoring CLI Sessions, page 5-7
- Monitoring DHCP Statistics, page 5-8
- Monitoring WLANs, page 5-9

Monitoring System Summary

This page displays a summary of the controller parameters with a graphic displaying the status of the controller. The graphic of the front of the controller shows front-panel ports (click a port to go to **Monitor Controllers** > *IPaddr* > Ports > General for information about that port). You can find the links to alarms, events and access points details related to the controller.

To access this page:

- Choose **Monitor > Controllers** and click the applicable IP address.
- Choose **Monitor > Access Points**, click a list item under AP Name, and then click **Registered Controller**.
- Choose **Configure > Access Points**, choose a list item under AP Name, then click **Registered Controller**.

Click **Controllers** in the page title to view a list of all the controllers. See the "Viewing List of Controllers" section on page 5-2.

The following parameters are displayed:

Table 5-3 Monitoring System Summary

Parameter	Description
General	
IP Address	Local network IP address of the controller management interface.
Name	User-defined name of the controller.
Device Type	Type of controller.
UP Time	Time in days, hours and minutes since the last reboot.
System Time	Time used by the controller.
Internal Temperature	The temperature of the controller.
Location	User-defined physical location of the controller.
Contact	Contact person or the owner of the controller.
Total Client Count	Total number of clients currently associated with the controller.
Current CAPWAP Transport Mode	Control and Provisioning of Wireless Access Points protocol (CAPWAP) transport mode. Communications between controllers and access points. Selections are Layer 2 or Layer 3.
Power Supply One	If the power supply is available and operation. This is only for 4400 series controller.
Power Supply Two	If the power supply is available and operation. This is only for 4400 series controller.
Inventory	
Software Version	The operating system release.version.dot.maintenance number of the code currently running on the controller.
Emergency Image Version	An image version of the controller.
Description	Description of the inventory item.
Model No	Specifies the machine model as defined by the Vital Product Data.

Table 5-3 Monitoring System Summary

Parameter	Description
Serial No	Unique serial number for this controller.
Burned-in MAC Address	The burned-in MAC address for this controller.
Number of APs Supported	The maximum number of access points supported by the controller.
Gig Ethernet/Fiber Card	Displays the presence or absence of the optional 1000BASE-T/1000BASE-SX GigE card.
Crypto Card One	Displays the presence or absence of an enhanced security module which enables IPSec security and provides enhanced processing power. **Note** By default, enhanced security module is not installed on a controller. Maximum number of crypto cards that can be installed on a Cisco Wireless LAN controller: – Cisco 2000 Series—None – Cisco 4100 Series—One – Cisco 4400 Series—Two
Crypto Card Two	Displays the presence or absence of a second enhanced security module.
GIGE Port(s) Status	Up or Down. Click to review the status of the port.
Unique Device Identifier (UDI)	
Name	Product type. Chassis for controller and Cisco AP for access points.
Description	Description of controller and may include number of access points.
Product ID	Orderable product identifier.
Version ID	Version of product identifier.
Serial No	Unique product serial number.
Utilization	
CPU Utilization	Displays a graph of the maximum, average, and minimum CPU utilization over the specified amount of time.
Memory Utilization	Displays a graph of the maximum, average, and minimum Memory utilization over the specified amount of time.

Monitoring Spanning Tree Protocol

The Spanning Tree Protocol (STP) is a link management protocol. Cisco WLAN Solution implements the IEEE 802.1D standard for media access control bridges.

Spanning tree algorithm provides redundancy while preventing undesirable loops in a network that are created by multiple active paths between stations. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail.

You can access this page in the following ways:

- Choose **Monitor > Controllers**, select an IP address, and choose **System** > **Spanning Tree Protocol** from the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **System** > **Spanning Tree Protocol** from the left sidebar menu.

Note The controllers that do not support Spanning Tree Protocol are WISM, 2500, 5500, 7500 and SMWLC.

This page enables you to view the following Spanning Tree Algorithm parameters:

Table 5-4 Spanning Tree Protocol Parameters

Parameter	Description
General	
Spanning Tree Specification	An indication of what version of the Spanning Tree Protocol is being run. IEEE 802.1D implementations will return 'IEEE 802.1D'. If future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version a new value will be defined.
Spanning Tree Algorithm	Specifies if this controller will participate in the Spanning Tree Protocol. May be enabled or disabled by selecting the corresponding line on the drop-down list entry field. The factory default is disabled.
Priority	The value of the writable portion of the Bridge ID, that is, the first two octets of the (8 octet long) Bridge ID. The other (last) 6 octets of the Bridge ID are given by the value of Bridge MAC Address. The value may be specified as a number between 0 and 65535. The factory default is 32768.
STP Statistics	
Topology Change Count	The total number of topology changes detected by this bridge since the management entity was last reset or initialized.
Time Since Topology Changed	The total number of topology changes detected by this bridge since the management entity was last reset or initialized.
Designated Root	The bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol as executed by this node. This value is used as the Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
Root Cost	The cost of the path to the root as seen from this bridge.
Root Port	The port number of the port which offers the lowest cost path from this bridge to the root bridge.

Table 5-4 Spanning Tree Protocol Parameters

Parameter	Description
Maximum Age (seconds)	The value that all bridges use for MaxAge when this bridge is acting as the root. **Note** The 802.1D-1990 specifies that the range for this parameter is related to the value of Stp Bridge Hello Time. The granularity of this timer is specified by 802.1D-1990 to be 1 second. Valid values are 6 through 40 seconds. The factory default is 20.
Hello Time (seconds)	The value that all bridges use for HelloTime when this bridge is acting as the root. The granularity of this timer is specified by 802.1D-1990 to be 1 second. Valid values are 1 through 10 seconds. The factory default is 2.
Forward Delay (seconds)	The value that all bridges use for ForwardDelay when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of Stp Bridge Maximum Age. The granularity of this timer is specified by 802.1D-1990 to be 1 second. An agent may return a badValue error if a set is attempted to a value which is not a whole number of seconds. Valid values are 4 through 30 seconds. The factory default is 15.
Hold Time (seconds)	The minimum time period to elapse between the transmission of Configuration BPDUs through a given LAN Port: at most one Configuration BPDU shall be transmitted in any Hold Time period.

Monitoring CLI Sessions

The CLI Sessions page for a controller can be accessed in the following ways:

- Choose **Monitor > Controllers**, click the applicable IP address, then choose **System** > **CLI Sessions** from the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then select **System > CLI Sessions** from the left sidebar menu.

This page provides a list of open command-line interface sessions. It details the following information:

Table 5-5 CLI Sessions Details

Parameter	Description
Session Index	Session identification.
Username	Login username.
Connection Type	Telnet or serial session.
Connection From	IP address of the client computer system.
Session Time	Elapsed active session time.
Idle Time	Elapsed inactive session time.

Monitoring DHCP Statistics

NCS provides DHCP server statistics for version 5.0.6.0 controllers or later. These statistics include information on the packets sent and received, DHCP server response information, last request timestamp.

To access this page, choose **Monitor > Controllers**, click the applicable IP address, then choose **System > DHCP Statistics** from the left sidebar menu.

The DHCP Statistics page provides the following information:

Table 5-6 DHCP Statistics

Parameter	Description
Server IP	Identifies the IP address of the server.
Is Proxy	Identifies whether or not this server is proxy.
Discover Packets Sent	Identifies the total number of packets sent intended to locate available servers.
Request Packets Sent	Identifies the total number of packets sent from the client requesting parameters from the server or confirming the correctness of an address.
Decline Packets	Identifies the number of packets indicating that the network address is already in use.
Inform Packets	Identifies the number of client requests to the DHCP server for local configuration parameters because the client already has an externally configured network address.
Release Packets	Identifies the number of packets that release the network address and cancel the remaining lease.
Reply Packets	Identifies the number of reply packets.
Offer Packets	Identifies the number of packets that respond to the discover packets with an offer of configuration parameters.
Ack Packets	Identifies the number of packets that acknowledge successful transmission.
Nak Packets	Identifies the number of packets that indicate that the transmission occurred with errors.
Tx Failures	Identifies the number of transfer failures that occurred.
Last Response Received	Provides a timestamp of the last response received.
Last Request Sent	Provides a timestamp of the last request sent.

Monitoring WLANs

Choose **Monitor > Controllers** and click a controller IP address, and choose **WLANs** from the left sidebar menu. This page enables you to view a summary of the wireless local access networks (WLANs) that you have configured on this controller:

Table 5-7 WLAN Details

Parameter	Description
WLAN ID	Identification number of the WLAN.
Profile Name	User-defined profile name specified when initially creating the WLAN. Profile Name is the WLAN name.
SSID	User-defined SSID name.
Security Policies	Security policies enabled on the WLAN.
No of Mobility Anchors	Mobility anchors are a subset of a mobility group specified as the anchor controllers for a WLAN.
Admin Status	Status of the WLAN is either enabled or disabled.
No. of Clients	Current number of clients currently associated with this WLAN.

Monitoring Ports

This section provides the detailed information regarding monitoring controller port parameters and contains the following topics:

- Monitoring General Ports, page 5-9
- Monitoring CDP Interface Neighbors, page 5-14

Monitoring General Ports

The Ports > General page provides information regarding physical ports on the selected controller. Click a port number to view details for that port. See the "Port Details" section on page 5-10 for more information.

General port information includes the following:

Table 5-8 General Ports

Parameter	Description
Port	Click the port number to view port details. See the "Port Details" section on page 5-10 for more information.
Physical Mode	Displays the physical mode of all ports. Selections include: – 100 Mbps Full Duplex – 100 Mbps Half Duplex – 10 Mbps Full Duplex – 10 Mbps Half Duplex
Admin Status	Displays the state of the port of either Enable or Disable.
STP State	Displays the STP state of the port of either Forwarding or Disabled.
Physical Status	Displays the actual port physical interface: – Auto Negotiate – Half Duplex 10 Mbps – Full Duplex 10 Mbps – Half Duplex 100 Mbps – Full Duplex 100 Mbps – Full Duplex 1 Gbps
Link Status	Red (down/failure), Yellow (alarm), Green (up/normal).

To access the Monitor > Ports > General page, do one of the following:

- Choose **Configure > Controllers**, click the applicable IP address. From the left sidebar menu, choose **General** under Ports.
- Choose **Monitor > Controllers,** click the applicable, and click a port to access this page.
- Choose **Monitor > Access Points** and click a list item under AP Name, click **Registered Controller**, then click a port to access this page.
- Choose **Monitor > Clients** and click a list item under AP Name, then click **Registered Controller**, then click a port to access this page.

Port Details

Note Click **Alarms** to open the Monitor Alarms page. See the "Monitoring Alarms" section on page 5-125 for more information.
Click **Events** to open the Monitor Events page. See the "Monitoring Events" section on page 5-142 for more information.

The Port Detail page includes the following information:

Table 5-9 Port Details

Parameter	Description
Interface	
Operational Status	Displays the operational status of the controller: Options are UP or DOWN.
Unknown Protocol Packets	The number of packets of unknown type which were received from this server on this port.
Traffic (Received and Transmitted)	
Total Bytes	The total number of packets received.
Packets	The total number of packets (including bad packets) received that were within the indicated octet range in length (excluding framing bits but including FCS octets). Ranges include: – 64 Octets – 65-127 Octets – 128-255 Octets – 256-511 Octets – 512-1023 Octets – 1024-1518 Octets
Packets (Received and Transmitted)	
Total	Total number of packets received/transmitted.
Unicast Packets	The number of subnetwork-unicast packets delivered/sent to a higher-layer protocol.
Broadcast Packets	The total number of packets received/sent that were directed to the broadcast address.
Packets Discarded	Packets Discarded (Received/Transmitted): The number of inbound/outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Errors in Packets	The total number of packets received that were with errors.
Received packets with MAC errors	

Table 5-9 Port Details

Parameter	Description
Jabbers	The total 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 non-integral number of octets (Alignment Error). **Note** This definition of jabber is different than 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 and 150 ms.
Fragments/Undersize	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
Alignment Errors	The total 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 non-integral number of octets.
FCS Errors	The total 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.
Transmit discards	
Single Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Deferred Transmissions	A count of frames for which transmission on a particular interface fails due to deferred transmissions.
Late Collisions	A count of frames for which transmission on a particular interface fails due to late collisions.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.
Ether Stats	

Table 5-9 Port Details

Parameter	Description
CRC Align Errors	The number of incoming packets with the Checksum (FCS) alignment error. This represents a count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. Received frames for which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
Undersize Packets	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
Oversize Packets	The total 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.
Ether Stats Collisions	The number of packets with collision errors.
SQE Test Errors	Signal Quality Error Test errors (that is, Heartbeat) during transmission. This tests the important collision detection electronics of the transceiver, and lets the Ethernet interface in the computer know that the collision detection circuits and signal paths are working correctly. The errors indicate a count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLong property, the AlignmentErrors property, or the FCSErrors property. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted.

Table 5-9 Port Details

Parameter	Description
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions property, the ExcessiveCollisions property, or the CarrierSenseErrors property. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.
Carrier Sense Errors	The Carrier Sense detects the presence of a carrier. The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface.
Too Long Frames	A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the FrameTooLong status is returned by the MAC layer to the LLC (or other MAC user). Received frames for which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.

Monitoring CDP Interface Neighbors

To access the Monitor CDP Interface Neighbors page, follow these steps:

Step 1 Choose **Monitor > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **CDP Interface Neighbors** (under the **Port** heading).

Step 4 The CDP Interface Neighbors page provides the following information:

Table 5-10 CDP Interface Neighbor Details

Parameter	Description
Local Interface	Local Port information.
Neighbor Name	The name of each CDP neighbor.
Neighbor Address	The IP address of each CDP neighbor.
Neighbor Port	The port used by each CDP neighbor for transmitting CDP packets.
Capability	The functional capability of each CDP neighbor.
Platform	The hardware platform of each CDP neighbor device.
Duplex	Indicates Full Duplex or Half Duplex.
Software Version	The software running on the CDP neighbor.

Monitoring Controller Security

This section provides the detailed information regarding monitoring controller security and contains the following topics:

- Monitoring RADIUS Authentication, page 5-15
- Monitoring RADIUS Accounting, page 5-17
- Monitoring Management Frame Protection, page 5-19
- Monitoring Rogue AP Rules, page 5-20
- Monitoring Guest Users, page 5-22

Monitoring RADIUS Authentication

The RADIUS authentication page displays RADIUS authentication server information and enables you to add or delete a RADIUS authentication server.

To access this page, do one of the following:

- Choose **Monitor > Controllers**, click the applicable IP address, then choose **Radius Authentication** from the Security section of the left sidebar menu.
- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **Radius Authentication** from the Security section of the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **Radius Authentication** from the Security section of the left sidebar menu.

The following information is displayed:

Table 5-11 RADIUS authentictaion details

Parameter	Description
RADIUS Authentication Servers	
Server Index	Access priority number for RADIUS servers. Up to four servers can be configured, and controller polling of the servers starts with Index 1, Index 2 second, and so forth. Index number is based on when the RADIUS server is added to the controller.
IP Address	The IP address of the RADIUS server.
Ping	Click to icon to ping the RADIUS Server from the controller to verify the link.
Port	Controller port number for the interface protocols.
Admin Status	Indicates whether the server is enabled or disabled.
Authentication Server Statistics	
Msg Round Trip Time	The time interval (in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
First Requests	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
Retry Requests	The number of RADIUS Authentication-Request packets retransmitted to this RADIUS authentication server.
Accept Responses	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
Reject Responses	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
Challenge Responses	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
Malformed Msgs	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or unknown types are not included as malformed access responses.

Table 5-11 RADIUS authentictaion details

Parameter	Description
Pending Requests	The 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 or Access-Challenge, a timeout, or retransmission.
Bad Authentication Msgs	The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.
Timeouts Requests	The 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	The number of RADIUS packets of unknown type which were received from this server on the authentication port.
Other Drops	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

Monitoring RADIUS Accounting

You can access this page by any of the following ways:

- Choose **Monitor > Controllers** and click the applicable IP address, then choose **Radius Accounting** from the Security section of the left sidebar menu.
- Choose **Monitor > Clients** and click a list item under AP Name, click **Registered Controller**, then choose **Radius Accounting** from the Security section of the left sidebar menu.
- Choose **Monitor > Maps**, click an item in the **Name** column, click an access point icon, click **Controller**, then choose **Radius Accounting** from the Security section of the left sidebar menu.
- Choose **Configure > Access Points** and select a list item under AP Name, click **Registered Controller**, then choose **Radius Accounting** from the Security section of the left sidebar menu.

This page displays RADIUS accounting server information and statistics:

Table 5-12 RADIUS Accoungting Details

Parameter	Description
RADIUS Accounting Server	
Server Index	Access priority number for RADIUS servers. Up to four servers can be configured, and controller polling of the servers starts with Index 1, Index 2 second, and so forth. Index number is based on when the RADIUS server is added to the controller.
IP Address	The IP address of the RADIUS server.
Ping	Click to icon to ping the RADIUS Server from the controller to verify the link.
Port	The Port of the RADIUS Server.
Admin Status	Indicates whether the server is enabled or disabled.
Accounting Statistics	
Msg Round Trip Time	The time interval (in milliseconds) between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
First Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Retry Requests	The 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	The number of RADIUS packets received on the accounting port from this server.
Malformed Msgs	The 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 Authentication Msgs	The number of RADIUS Accounting-Response packets which contained invalid authenticators received from this server.

Table 5-12 RADIUS Accoungting Details

Parameter	Description
Pending Requests	The 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.
Timeouts Requests	The 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	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
Other Drops	The number of RADIUS packets which were received from this server on the accounting port and dropped for some other reason.

Monitoring Management Frame Protection

This page displays the Management Frame Protection (MFP) summary information. MFP provides for the authentication of 802.11 management frames. Management frames can be protected to detect adversaries who are invoking denial of service attacks, flooding the network with probes, interjecting as rogue access points, and affecting the network performance by attacking the QoS and radio measurement frames.

If one or more of the WLANs for the controller has MFP enabled, the controller sends each registered access point a unique key for each BSSID the access point uses for those WLANs. Management frames sent by the access point over the MFP enabled WLANs will be signed with a Frame Protection Information Element (IE). Any attempt to alter the frame invalidates the message causing the receiving access point configured to detect MFP frames to report the discrepancy to the WLAN controller.

Access this page in one of the following ways:

- Choose **Monitor > Controllers**. From the Controllers > Search Results page, click the applicable IP Address, then choose **Management Frame Protection** from the Security section of the left sidebar menu.
- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **Management Frame Protection** from the Security section of the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **Management Frame Protection** from the Security section of the left sidebar menu.

The following parameters are displayed:

Table 5-13 MFP Details

Parameter	Description
General	
Management Frame Protection	Indicates if infrastructure MFP is enabled globally for the controller.
Controller Time Source Valid	The Controller Time Source Valid field indicates whether the controller time is set locally (by manually entering the time) or through an external source (such as NTP server). If the time is set by an external source, the value of this field is "True." If the time is set locally, the value is "False." The time source is used for validating the timestamp on management frames between access points of different controllers within a mobility group.
WLAN Details	
WLAN ID	The WLAN ID, 1 through 17.
WLAN Name	User-defined profile name when initially creating the WLAN. Both the SSID name and profile name are user-defined. The WLAN name is same as the profile name.
MFP Protection	Management Frame Protection is either enabled or disabled.
Status	Status of the WLAN is either enabled or disabled.
AP Details	
AP Name	Operator defined name of access point.
MFP Validation	Management Frame Protection is enabled or disabled.
Radio	802.11a or 802.11b/g.
Operation Status	Displays the operational status of the: either UP or DOWN.
Protection	Full (All Frames).
Validation	Full (All Frames).

Monitoring Rogue AP Rules

Rogue AP rules automatically classify rogue access points based on criteria such as authentication type, matching configured SSIDs, client count, and RSSI values. NCS applies the rogue access point classification rules to the controllers and respective access points.

These rules can limit a rogue appearance on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time).

Rogue AP Rules also help reduce false alarms.

Note Rogue classes include the following types:
Malicious Rogue—A detected access point that matches the user-defined malicious rules or has been manually moved from the Friendly AP category.
Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined friendly rules.
Unclassified Rogue—A detected access point that does not match the malicious or friendly rules.

Choose **Monitor > Controllers**. From the Controllers > Search Results page, click the applicable IP Address, then choose **Rogue AP Rules** from the Security section of the left sidebar menu.

The **Rogue AP Rules** page provides a list of all rogue access point rules currently applied to this controller.

The following information is displayed for rogue access point rules:

- Rogue AP Rule name—Click the link to view Rogue AP Rule details.
- Rule Type—Malicious or Friendly.
  - Malicious Rogue—A detected access point that matches the user-defined Malicious rules or has been manually moved from the Friendly AP category.
  - Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined Friendly rules.
- Priority—Indicates the priority level for this rogue AP rule.

Note See the "Configuring a Rogue AP Rules Template" section on page 11-78 for more information on Rogue AP Rules.

Rogue AP Rules Details

The Rogue AP Rules Details page displays the following information:

Table 5-14 Rogue AP Rule Details

Parameter	Description
Rule Name	Name of the rule.
Rule Type	Malicious or Friendly – Malicious Rogue—A detected access point that matches the user-defined Malicious rules or has been manually moved from the Friendly AP category. – Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined Friendly rules.

Table 5-14 Rogue AP Rule Details

Parameter	Description
Match Type	Match any or match all conditions.
Enabled Rule Conditions	Indicates all enabled rule conditions including: – Open Authentication – Match Managed AP SSID – Match User Configured SSID – Minimum RSSI – Time Duration – Minimum Number Rogue Clients

Note See the "Configuring a Rogue AP Rules Template" section on page 11-78 for more information on Rogue AP Rules.

Monitoring Guest Users

Choose **Monitor > Controllers**. From the Controllers > Search Results page, click the applicable IP Address, then choose **Guest Users** from the Security section of the left sidebar menu.

NCS allows you to monitor guest users from the Guest Users page as well as from the NCS home page.

The Guest Users page provides a summary of the guest access deployment and network use.

The following information is displayed for guest users currently associates on the network:

Table 5-15 Guest User Details

Parameter	Description
Guest User Name	Indicates the guest user login name.
Profile	Indicates the profile to which the guest user is connected.
Lifetime	Indicates the length of time that the guest user account is active. Length of time appears in days, hours, and minutes or as Never Expires.
Start Time	Indicates when the guest user account was activated.
Remaining Lifetime	Indicates the remaining time for the guest user account.
Role	Indicates the designated user role.
First Logged in at	Indicates the date and time of the user first log in.
Number of logins	Indicates the total number of log ins for this guest user.
Description	User-defined description of the guest user account for identification purposes.

Monitoring Controllers Mobility

Monitoring Mobility Stats

The Mobility Stats page displays the statistics for mobility group events.

Access this page in one of the following ways:

- Choose **Monitor > Controllers** and click the applicable IP address, then choose **Mobility Stats** from the Mobility section of the left sidebar menu.
- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **Mobility Stats** from the Mobility section of the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **Mobility Stats** from the Mobility section of the left sidebar menu.

The following parameters are displayed:

Table 5-16 Mobility Stats

Parameter	Description
Global Mobility Statistics	
Rx Errors	Generic protocol packet receive errors, such as packet too short or format incorrect.
Tx Errors	Generic protocol packet transmit errors, such as packet transmission fail.
Responses Retransmitted	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 is a count of the response resends.
Handoff Requests Received	Total number of handoff requests received, ignored or responded to.
Handoff End Requests	Total number of handoff end requests received. These are sent by the Anchor or the Foreign to notify the other about the close of a client session.
State Transitions Disallowed	PEM (policy enforcement module) has denied a client state transition, usually resulting in the handoff being aborted.
Resource Unavailable	A necessary resource, such as a buffer, was unavailable, resulting in the handoff being aborted.
Mobility Responder Statistics	
Handoff Requests Ignored	Number of handoff requests/client announces that were ignored. The controller simply 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 sec).

Table 5-16 Mobility Stats

Parameter	Description
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 has moved from a foreign controller to controller on the same subnet as the current anchor.
Mobility Initiator Statistics	
Handoff Requests Sent	Number of clients that have associated with 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 Denies 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. Handoff was received from another foreign and the new controller is requesting the anchor 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 transfers that were received by the current anchor.

Monitoring Controller 802.11a/n

This section provides detailed information regarding monitoring 802.11a/n parameters and contains the following topics:

- Monitoring 802.11a/n Parameters, page 5-25
- Monitoring 802.11a/n RRM Groups, page 5-26

Monitoring 802.11a/n Parameters

Access this parameters page in one of the following ways:

- Choose **Monitor > Controllers** and click the applicable IP address, then choose **Parameters** from the 802.11a/n section of the left sidebar menu.
- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **Parameters** from the 802.11a/n section of the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **Parameters** from the 802.11a/n section of the left sidebar menu.

This page displays the following 802.11a/n parameters:

Table 5-17 802.11 a/n Parameters

Parameter	Description
MAC Operation Parameters	
RTS Threshold	Indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed. **Note** An RTS/CTS handshake is performed at the beginning of any frame exchange sequence where the MPDU is a data or management type, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute higher than the maximum MSDU size turns off the RTS/CTS handshake for data or management type frames transmitted by this STA. Setting this attribute to zero turns on the RTS/CTS handshake for all transmitted data or management type frames.
Short Retry Limit	The maximum number of transmission attempts of a frame (less than or equal to dot11RTSThreshold) made before a failure condition is indicated. The default value is 7.
Long Retry Limit	The maximum number of transmission attempts of a frame (greater than dot11RTSThreshold) made before a failure condition is indicated. The default value is 4.
Max Tx MSDU Lifetime	The elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU are terminated. The default value is 512.

Table 5-17 802.11 a/n Parameters

Parameter	Description
Max Rx Lifetime	The elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU are terminated. The default value is 512.
Physical Channel Parameters	
TI Threshold	The threshold being used to detect a busy medium (frequency). CCA shall report a busy medium upon detecting the RSSI above this threshold.
Channel Agility Enabled	Physical channel agility functionality is or is not implemented.
Station Configuration Parameters	
Medium Occupancy Limit	Indicates the maximum amount of time, in TU, that a point coordinator may control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.
CFP Period	The number of DTIM intervals between the start of CFPs. It is modified by MLME-START.request primitive.
CFP Max Duration	The maximum duration of the CFP in TU that may be generated by the PCF. It is modified by MLME-START.request primitive.
CF Pollable	When this attribute is implemented, it indicates that 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	Specifies whether CFP is requested by the client.
DTIM Period	The number of beacon intervals that shall elapse between transmission of Beacon frames containing a TIM element whose DTIM Count field is 0. This value is transmitted in the DTIM Period field of Beacon frames.

Monitoring 802.11a/n RRM Groups

Access the RRM Grouping page in one of the following ways:

- Choose **Monitor > Controllers** and click the applicable IP address, then choose **Grouping** or **WPS Grouping** from the 802.11a/n section of the left sidebar menu.
- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **RRM Grouping** or **WPS Grouping** from the 802.11a/n section of the left sidebar menu.

- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **RRM Grouping** or **WPS Grouping** from the 802.11a/n section of the left sidebar menu.

This page displays the following 802.11a RRM groups parameters:

Table 5-18 802.11 a/n RRM Groups

Parameter	Description
802.11a Grouping Control	
Grouping Mode	Dynamic grouping has two modes: on and off. When the grouping is off, no dynamic grouping occurs. Each controller optimizes only its own access point's parameters. When grouping is on, the controller forms groups and elects leaders to perform better dynamic parameter optimization.
Grouping Role	There are five grouping roles: – None—This grouping role appears when the RF Group Mode is configured as Off. – Auto-Leader—This grouping role appears when the RF Group Mode is configured as Automatic and the controller is elected as a leader by the automatic grouping algorithm. – Auto-Member—This grouping role appears when the RF Group Mode is configured as Automatic and the controller is selected as a member by the automatic grouping algorithm. – Static-Leader—This grouping role appears when the RF Group Mode is configured as Leader. – Static-member—This grouping role appears when the RF Group Mode is configured as automatic and the controller joins the leader as a result of the join request from the leader.
Group Leader IP Address	This is the IP address of the group leader.
Group Leader MAC Address	This is the MAC address of the group leader for the group containing this controller.
Is 802.11a Group Leader	Yes, if this controller is the group leader or No if the controller is not the group leader.
Last Update Time (secs)	The elapsed time since the last group update in seconds. This is only valid if this controller is a group leader.

Table 5-18 802.11 a/n RRM Groups

Parameter	Description
Group Update Interval (secs)	When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. Grouping algorithm will also run when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. Default value is 3600 seconds.
Group Members	
Group Member Name	Name of group member(s).
Group Member IP Address	IP address of group member(s).
Member Join Reason	Current state of the member(s).

Monitoring Controllers 802.11b/g/n

This section provides the detailed information regarding monitoring 802.11b/g/n parameters and contains the following topics:

- Monitoring 802.11b/g/n Parameters, page 5-28
- Monitoring 802.11b/g/n RRM Groups, page 5-30

Monitoring 802.11b/g/n Parameters

Access this parameters page in one of the following ways:

- Choose **Monitor > Controllers** and click the applicable IP Address, then choose **Parameters** from the 802.11b/g/n section of the left sidebar menu.
- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **Parameters** from the 802.11b/g/n section of the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **Parameters** from the 802.11b/g/n section of the left sidebar menu.

This page displays the following 802.11b/g parameters:

Table 5-19 802.11 b/g/n Parameters

Parameter	Description
MAC Operation Parameters	
RTS Threshold	Indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed. **Note** An RTS/CTS handshake is performed at the beginning of any frame exchange sequence where the MPDU is a data or management type, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute higher than the maximum MSDU size turns off the RTS/CTS handshake for data or management type frames transmitted by this STA. Setting this attribute to zero turns on the RTS/CTS handshake for all transmitted data or management type frames.
Short Retry Limit	The maximum number of transmission attempts of a frame (less than or equal to dot11RTSThreshold) made before a failure condition is indicated. The default value is 7.
Long Retry Limit	The maximum number of transmission attempts of a frame (greater than dot11RTSThreshold) made before a failure condition is indicated. The default value is 4.
Max Tx MSDU Lifetime	The elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU are terminated. The default value is 512.
Max Rx Lifetime	The elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU are terminated. The default value is 512.
Physical Channel Parameters	
TI Threshold	The threshold being used to detect a busy medium (frequency). CCA shall report a busy medium upon detecting the RSSI above this threshold.
Channel Agility Enabled	Physical channel agility functionality is or is not implemented.
Station Configuration Parameters	

Table 5-19 802.11 b/g/n Parameters

Parameter	Description
Medium Occupancy Limit	Indicates the maximum amount of time, in TU, that a point coordinator may control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.
CFP Period	The number of DTIM intervals between the start of CFPs. It is modified by MLME-START.request primitive.
CFP Max Duration	The maximum duration of the CFP in TU that may be generated by the PCF. It is modified by MLME-START.request primitive.
CF Pollable	When this attribute is implemented, it indicates that 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	Specifies whether CFP is requested by the client.
DTIM Period	The number of beacon intervals that shall elapse between transmission of Beacon frames containing a TIM element whose DTIM Count field is 0. This value is transmitted in the DTIM Period field of Beacon frames.

Monitoring 802.11b/g/n RRM Groups

Access the RRM Group page in one of the following ways:

- Choose **Monitor > Controllers** and click the applicable IP address, then choose **RRM Grouping** or **WPS Grouping** from the 802.11b/g/n section of the left sidebar menu.
- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **RRM Grouping** or **WPS Grouping** from the 802.11b/g/n section of the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **RRM Grouping** or **WPS Grouping** from the 802.11b/g/n section of the left sidebar menu.

This page displays the following 802.11b/g RRM groups parameters:

Table 5-20 802.11 b/g/n RRM groups

Parameter	Description
802.11 b/g/n Grouping Control	
Grouping Mode	Dynamic grouping has two modes: on and off. When the grouping is off, no dynamic grouping occurs. Each controller optimizes only its own access point's parameters. When grouping is on, the controller forms groups and elects leaders to perform better dynamic parameter optimization.
Grouping Role	There are five grouping roles: – None—This grouping role appears when the RF Group Mode is configured as Off. – Auto-Leader—This grouping role appears when the RF Group Mode is configured as Automatic and the controller is elected as a leader by the automatic grouping algorithm. – Auto-Member—This grouping role appears when the RF Group Mode is configured as Automatic and the controller is selected as a member by the automatic grouping algorithm. – Static-Leader—This grouping role appears when the RF Group Mode is configured as Leader. – Static-member—This grouping role appears when the RF Group Mode is configured as automatic and the controller joins the leader as a result of the join request from the leader.
Group Leader IP Address	This is the IP address of the group leader.
Group Leader MAC Address	This is the MAC address of the group leader for the group containing this controller.
Is 802.11a Group Leader	Yes, if this controller is the group leader or No if the controller is not the group leader.
Last Update Time (secs)	The elapsed time since the last group update in seconds. This is only valid if this controller is a group leader.

Table 5-20 802.11 b/g/n RRM groups

Parameter	Description
Group Update Interval (secs)	When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. Grouping algorithm will also run when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. Default value is 3600 seconds.
Group Members	
Group Member Name	Name of group member(s).
Group Member IP Address	IP address of group member(s).
Member Join Reason	Current state of the member(s).

Monitoring Switches

Choose **Monitor > Switches** to view the detailed information about the switches. The following sections provide more detailed information regarding monitoring switches:

- Searching Switches, page 5-32
- Viewing List of Switches, page 5-33
- Monitoring Switch System Parameters, page 5-33
- Monitoring Switch Interfaces, page 5-39
- Monitoring Switch Clients, page 5-41

Searching Switches

Use the NCS search feature to find specific switches or to create and save custom searches.

You can configure the following parameters when performing an advanced search for switches (see Table 5-21):

Table 5-21 Search Switches Parameters

Parameter	Options
Search for Switches by	Choose All Switches, IP Address, or Switch Name. You can use wildcards (*). For example, if you select IP Address and enter `172*`, NCS returns all switches that begin with IP address 172.
Items per page	Select the number of switches to return per page.

See one of the following topics for additional information:

- Using the Search Feature, page 2-33
- Quick Search, page 2-33

- Advanced Search, page 2-34
- Saved Searches, page 2-46

Viewing List of Switches

Choose **Monitor > Switches** to view a list of switches. From this page you can view a summary of switches including the default information shown in Table 5-22:

Table 5-22 Viewing List of Switches

Parameter	Description
IP Address	The IP address assigned to the switch. Click a list item to view access point details.
Device Name	Name of the switch.
Device Type	Type of switch.
Reachability Status	Indicates OK if the switch is reachable or Unreachable if the switch is not reachable.
Endpoint Count	Number of endpoints on the switch.

Configuring the Switch List Page

The **Edit View** page allows you to add, remove, or reorder columns in the Switches table.

To edit the available columns in the table, follow these steps:

Step 1 Choose **Monitor > Switches**.

Step 2 Click the **Edit View** link.

Step 3 To add an additional column to the table, click to highlight the column heading in the left column. Click **Show** to move the heading to the right column. All items in the right column are displayed in the table.

Step 4 To remove a column from the table, click to highlight the column heading in the right column. Click **Hide** to move the heading to the left column. All items in the left column are not displayed in the table.

Step 5 Use the **Up/Down** buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click **Up** or **Down** to move it higher or lower in the current list.

Step 6 Click **Reset** to restore the default view.

Step 7 Click **Submit** to confirm the changes.

Monitoring Switch System Parameters

Choose **Monitor > Switches**, then click an IP address under the IP Address column to view details about the switch. This section provides the detailed information regarding each switch details page and contains the following topics:

- Viewing Switch Summary Information, page 5-34
- Viewing Switch Memory Information, page 5-35

- Viewing Switch Environment Information, page 5-35
- Viewing Switch Module Information, page 5-36
- Viewing Switch VLAN Information, page 5-36
- Viewing Switch VTP Information, page 5-36
- Viewing Switch Physical Ports Information, page 5-37
- Viewing Switch Sensor Information, page 5-37
- Viewing Switch Spanning Tree Information, page 5-38
- Viewing Switch Stacks Information, page 5-39
- Viewing Switch NMSP and Location Information, page 5-39

Viewing Switch Summary Information

Choose **Monitor > Switches**, then click an IP address under the IP Address column to view details about the switch. Table 5-23 describes the summary information that is displayed.

Table 5-23 Viewing Switches Summary Information

General	
IP Address	IP address of the switch.
Device Name	Name of the switch.
Device Type	Switch type.
Up Time	Time since last reboot.
System Time	Time on the switch.
Reachability Status	which can be: • Reachable • Unreachable
Location	Location of the switch.
Contact	Contact name for the switch.
Cisco Identity Capable	Specifies if the switch is identity-capable.
Location Capable	Specifies if the switch is capable of storing the location information.
CPU Utilization	Displays a graph of the maximum, average, and minimum CPU utilization over the specified amount of time.
Unique Device Identifier (UDI)	
Name	Product type.
Description	Description of UDI.
Product ID	Orderable product identifier.
Version ID	Version of product identifier.
Serial Number	Unique product serial number.
Inventory	
Software Version	Version of software currently running on the switch.
Model No.	Model number of the switch.

Table 5-23 Viewing Switches Summary Information (continued)

Port Summary	
Number of Ports Up	Number of ports up on the switch.
Number of Ports Down	Number of ports down on the switch.
Memory Utilization	Displays a graph of the maximum, average, and minimum memory utilization over the specified amount of time.

Related Topic

- Monitoring Switch Interfaces, page 5-39

Viewing Switch Memory Information

Choose **Monitor > Switches**, then click an IP address under the IP Address column to view details about the switch. From the System menu, choose **Memory**. Table 5-24 describes the memory information that is displayed.

Table 5-24 Viewing Switches Memory Information

Memory Pool	
Type	Type of memory.
Name	Name assigned to the memory pool.
Used (MB)	Amount of memory (in MB) used.
Free (MB)	Amount of memory (in MB) available.

Viewing Switch Environment Information

Choose **Monitor > Switches**, then click an IP address under the IP Address column to view details about the switch. From the System menu, choose **Environment**. Table 5-25 describes the environment information that is displayed.

Table 5-25 Viewing Switches Environment Information

Power Supply	
Model Name	Model name of the power supply.
Description	Description of the power supply.
Operational Status	Status of the associated power supply, which can be • Green—Power supply is operational. • Red—Power supply is inoperable.
Manufacturer Name	Name of the power supply manufacturer.
Free	Power supply free slots.
Vendor Equipment Type	Description of vendor equipment type.
Fans	
Name	Name of fan.

Table 5-25 Viewing Switches Environment Information

Description	Description of fan.
Operational Status	Status of the fan which can be • Green—Fan is operational. • Red—Fan is inoperable.
Vendor Equipment Type	Description of vendor equipment type.
Serial Number	Serial number of the fan.

Viewing Switch Module Information

Choose **Monitor > Switches**, then click an IP address under the IP Address column to view details about the switch. From the System menu, choose **Modules**. Table 5-26 describes the module information that is displayed.

Table 5-26 Viewing Switches Modules Information

Modules	
Product Name	Name of the module.
Physical Location	Location where the module is contained.
Number of Ports	Number of ports supported by the module.
Operational State	Operational status of the module.
Equipment Type	Type of equipment.
Inline Power Capable	Specifies whether the module has inline power capability.

Viewing Switch VLAN Information

Choose **Monitor > Switches**, then click an IP address under the IP Address column to view details about the switch. From the System menu, choose **VLANs**. Table 5-27 describes the VLAN information that is displayed.

Table 5-27 Viewing Switches VLANs Information

VLANs	
VLAN ID	ID of the VLAN.
VLAN Name	Name of the VLAN.
VLAN Type	Type of VLAN.

Viewing Switch VTP Information

Choose **Monitor > Switches**, then click an IP address under the IP Address column to view details about the switch. From the System menu, choose **VTP**. Table 5-28 describes the VTP information that is displayed.

Table 5-28 Viewing Switches VTP Information

VTP	
VTP Domain Name	Name of the VTP domain.
VTP Version	Version of VTP in use.
VTP Mode	The VTP mode, which can be: • Client • Server • Transparent—Does not generate or listen to VTP messages, but forwards messages. • Off—Does not generate, listen to, or forward any VTP messages.
Pruning Enabled	Specifies whether VTP pruning is enabled.

Viewing Switch Physical Ports Information

Choose **Monitor > Switches**, then click an IP address under the IP Address column to view details about the switch. From the System menu, choose **Physical Ports**. Table 5-29 describes the physical ports information that is displayed.

Table 5-29 Viewing Switches Physical Ports Information

Physical Ports	
Port Name	Name of the physical port.
Port Description	Description of the physical port.
Residing Module	Module on which the physical port resides.
Vendor Equipment Type	Description of vendor equipment type.

Viewing Switch Sensor Information

Choose **Monitor > Switches**, then click an IP address under the IP Address column to view details about the switch. From the System menu, choose **Sensors**. Table 5-30 describes the sensor information that is displayed.

Table 5-30 Viewing Switches Sensors Information

Sensors	
Sensor Name	Name of the sensor.
Sensor Description	Description of the sensor.
Type	Type of sensor.
Vendor Sensor Type	Description of vendor sensor type.
Equipment Name	Name of equipment.

Table 5-30 Viewing Switches Sensors Information

Precision	When in the range 1 to 9, Sensor Precision is the number of decimal places in the fractional part of a Sensor Value fixed-point number. When in the range -8 to -1, Sensor Precision is the number of accurate digits in a Sensor-Value fixed-point number.
Status	Operational status of the sensor.

Viewing Switch Spanning Tree Information

Choose **Monitor > Switches**, then click an IP address under the IP Address column to view details about the switch. From the System menu, choose **Spanning Tree**. Table 5-31 describes the spanning tree information that is displayed.

Table 5-31 Viewing Switches Spanning Tree Information

Spanning Tree	
STP Instance ID	ID of the STP. Click on a STP Instance ID to see the spanning tree details as described in Viewing Spanning Tree Details.
VLAN ID	ID of the VLAN.
Root Path Cost	Root cost of the path.
Designated Root	Forwarding port.
Bridge Priority	Priority of the bridge.
Root Bridge Priority	Priority number of the root bridge.
Max Age (sec)	STP timer value for maximum age (in seconds).
Hello Interval (sec)	STP timer value (in seconds).

Viewing Spanning Tree Details

Choose **Monitor > Switches**, then click an IP address under the IP Address column to view details about the switch. From the System menu, choose **Spanning Tree**, then click on an STP instance ID to see the spanning tree details as described in Table 5-32.

Table 5-32 Viewing Spanning Tree Details

Spanning Tree	
STP Port	Name of the STP port.
Port Role	Role of the port.
Port Priority	Priority number of the port.
Path Cost	Cost of the path.
Port State	State of the port.
Port Type	Type of port.

Viewing Switch Stacks Information

Choose **Monitor > Switches**, then click an IP address under the IP Address column to view details about the switch. From the System menu, choose **Stacks**. Table 5-33 describes the spanning tree information that is displayed.

Table 5-33 Viewing Switches Stacks Information

Stacks	
MAC Address	MAC address of the stack.
Role	Role of the stack, which can be: • Master—Stack master • Member—Active member of the stack • Not Member—Non-active stack member
Switch Priority	Priority number of the switch.
State	Current state of the stack.
Software Version	Software image running on the switch.

Viewing Switch NMSP and Location Information

You can view the NMSP and Location information for a switch using the System left side-bar menu.

To view the NMSP and Location information for a switch, choose **NCS** > **Monitor** > **Switches** > *Switch IP Address* > **System** > **NMSP and Location**.

The NMSP and Location page appears.

You can view the NMSP Status in the NMSP Status pane and Location information in the Location pane.

For more information on NMSP and Location, see the Configuring Switch NMSP and Location.

Monitoring Switch Interfaces

Choose **Monitor > Switches**, then click an IP address under the IP Address column. From the System menu, choose **Interfaces**, then select one of the following interfaces:

- Monitoring Switch Ethernet Interfaces
- Monitoring Switch IP Interfaces
- Monitoring Switch VLAN Interfaces
- Monitoring Switch EtherChannel Interfaces

Monitoring Switch Ethernet Interfaces

Choose **Monitor > Switches**, then click an IP address under the IP Address column. From the System menu, choose **Interfaces > Ethernet Interfaces**. Table 5-34 describes the Ethernet interface information that is displayed:

Table 5-34 Viewing Switch Ethernet Interfaces

Name	Name of the Ethernet interface. Click on an Ethernet interface name to see details as described in Monitoring Switch Ethernet Interface Details.
MAC Address	MAC address of the Ethernet interface.
Speed (Mbps)	Estimate of the Ethernet interface's current bandwidth in bits per second.
Operational Status	Current operational state of the Ethernet interface.
MTU	Size of the largest packet that can be sent/received on the interface.
Desired VLAN Mode	VLAN mode.
Access VLAN	VLAN on which the port is configured.

Monitoring Switch Ethernet Interface Details

Choose **Monitor > Switches**, then click an IP address under the IP Address column. From the System menu, choose **Interfaces > Ethernet Interfaces**, then click on an Ethernet interface name in the Name column. Table 5-35 describes the Ethernet interface detail information that is displayed:

Table 5-35 Viewing Switch Ethernet Interface Details

Ethernet Interfaces	
Name	Name of the Ethernet interface.
Admin Status	Administration status of the interface.
Duplex Mode	Duplex mode configured on the interface.
VLAN Switch Port	
Operational VLAN Mode	Specifies the operational mode of the VLAN switch port, which can be either an access port or a trunk port.
Desired VLAN Mode	VLAN mode, which can be truck, access, dynamic, or desirable.
Access VLAN	VLAN on which the port is configured.
Operational Truck Encapsulation	Trunk encapsulation, which can be *802.1Q* or *none*.
VLAN Trunk	
Native VLAN	Untagged VLAN on the trunk switch port.
Prune Eligible	Specifies whether VLANs on the trunk port can be pruned.
Allows VLANs	List of allowed VLANs on the trunk port.
Desired Trunking Encapsulation	Trunk encapsulation.
Trunking Encapsulation Negotiation	Specifies that the interface negotiate with the neighboring interface to become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring interface.

Monitoring Switch IP Interfaces

Choose **Monitor > Switches**, then click an IP address under the IP Address column. From the System menu, choose **Interfaces > IP Interfaces**. Table 5-36 describes the IP interface information that is displayed:

Table 5-36 Viewing Switch IP Interfaces

Interface	Name of the interface.
IP Address	IP address of the interface.
Address Type	Type of address (IPv4 or IPv6).

Monitoring Switch VLAN Interfaces

Choose **Monitor > Switches**, then click an IP address under the IP Address column. From the System menu, choose **Interfaces > VLAN Interfaces**. Table 5-37 describes the VLAN interface information that is displayed:

Table 5-37 Viewing Switch VLAN Interfaces

Port Name	Name of the VLAN port.
VLAN ID	ID of the VLAN port.
Operational Status	Current operational state of the VLAN interface.
Admin Status	Current administrative state of the VLAN interface.
Port Type	Type of VLAN port.
Maximum Speed (Mbps)	Maximum supported speed for the VLAN interface.
MTU	Size of the largest packet that can be sent/received on the VLAN interface.

Monitoring Switch EtherChannel Interfaces

Choose **Monitor > Switches**, then click an IP address under the IP Address column. From the System menu, choose **Interfaces > EtherChannel Interfaces**. Table 5-38 describes the EtherChannel interface information that is displayed:

Table 5-38 Viewing Switch EtherChannel Interfaces

Name	Name of the EtherChannel interface.
Channel Group ID	Numeric identifier for the EtherChannel.
Control Method	Protocol for managing the EtherChannel, which can be LACP or TAgP.
Actor Admin Key	Channel Identifier.
Number of (LAG) Members	Number of ports configured.

Monitoring Switch Clients

Choose **Monitor > Switches**, then click an IP address under the IP Address column. From the System menu, choose **Clients**. Table 5-38 describes the EtherChannel interface information that is displayed:

Table 5-39 Viewing Current Associated Client

IP Address	IP address of the client.
MAC Address	MAC address of the client.

Table 5-39 Viewing Current Associated Client

User Name	User Name of the client.
Vendor Name	Vendor Name of the client.
Map Location	Location of the client.
VLAN	VLAN on which the client is configured.
Interface	Interface on which the client is configured.
Association Time	Timestamp of the client association.
Authorization Profile Name	Authorization Profile Name stored.

Monitoring Access Points

This section provides access to the controller access points summary details. Use the main date area to access the respective access point details.

Choose **Monitor > Access Points** to access this page. This section provides more detailed information regarding monitoring access points and contains the following topics:

- Searching Access Points, page 5-42
- Viewing List of Access Points, page 5-43
- Generating a Report for Access Points, page 5-46
- Monitoring Access Points Details, page 5-56
- Monitoring Access Point Radio Details, page 5-68
- Monitoring Mesh Access Points, page 5-77
- Retrieving the Unique Device Identifier on Controllers and Access Points, page 5-83
- Monitoring Coverage Hole, page 5-84
- Monitoring Rogue Access Points, page 5-86
- Monitoring Adhoc Rogues, page 5-100
- Searching Rogue Clients Using Advanced Search, page 5-105
- Monitoring Rogue Access Point Location, Tagging, and Containment, page 5-107

Searching Access Points

Use the NCS Search feature to find specific access points or to create and save custom searches. See one of the following topics for additional information:

- Using the Search Feature, page 2-33
- Quick Search, page 2-33
- Advanced Search, page 2-34
- Saved Searches, page 2-46

Viewing List of Access Points

Choose **Monitor > Access Points** or perform an access point search to access this page.

This page enables you to view a summary of access points including the following default information:

Table 5-40 Access Point Search Results

Parameter	Description
AP Name Ethernet MAC	The name assigned to the access point. Click a list item to view access point details. See the "Monitoring Access Points Details" section on page 5-56 for more information.
IP Address	Local IP address of the access point.
Radio	Protocol of the rogue access point is 802.11a, 802.11b or 802.11g. Click a list item to view access point radio details. See the "Monitoring Access Point Radio Details" section on page 5-68 for more information.
Map Location	Click a list item to go to the location indicated on the list.
Controller	Click a list item to display a graphic and information about the controller. See the "Monitoring System Summary" section on page 5-4 for more information.
Client Count	Displays the total number of clients currently associated with the controller.
Admin Status	Displays the administration state of the access point as either enabled or disabled.
AP Mode	Displays the operational mode of the access point.
Oper Status	Displays the operational status of the Cisco WLAN Solution device, either Up or Down. If the admin status is disabled, the operation status is labeled as down and there will be no alarms.
Alarm Status	Alarms are color coded as follows: – Clear—No Alarm – Red—Critical Alarm – Orange—Major Alarm – Yellow—Minor Alarm **Note** This status is radio alarm status ONLY and does not includes the admin status in the operation status.

Configuring the Access Point List Display

To add, remove, or reorder columns in the table, click the **Edit View** link to go to the Edit View page. The following are optional access point parameters available for the search results:

Table 5-41 Edit View Search Results

Parameters	Description
AP Type	Indicates the type of access point (unified or autonomous).
Antenna Azim. Angle	Indicates the horizontal angle of the antenna.
Antenna Diversity	Indicates if antenna diversity is enabled or disabled. Antenna diversity refers to the access point sampling the radio signal from two integrated antenna ports to choose the preferred antenna.
Antenna Elev. Angle	Indicates the elevation angle of the antenna.
Antenna Gain	The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means 4 x 0.5 = 2 dBm of gain.
Antenna Mode	Indicates the antenna mode such as omni, directional, or non-applicable.
Antenna Name	Indicates the antenna name or type.
Audit Status	Indicates one of the following audit statuses: – Mismatch—Config differences were found between NCS and controller during the last audit. – Identical—No config differences were found during the last audit. – Not Available—Audit status is unavailable.
Base Radio MAC	Indicates the MAC address of the base radio.
Bridge Group Name	Indicates the name of the bridge group used to group the access points, if applicable.
CDP Neighbors	Indicates all directly connected Cisco devices.
Channel Control	Indicates whether the channel control is automatic or custom.
Channel Number	Indicates the channel on which the Cisco Radio is broadcasting.
Controller Port	Indicates the number of controller ports.
Google Earth Location	Indicates whether or not a Google Earth location is assigned and indicates the location.
Location	Indicates the physical location of the access point.

Table 5-41 Edit View Search Results

Parameters	Description
Node Hops	Indicates the number of hops between access points.
OfficeExtend AP	Specifies whether or not OfficeExtend access is enabled. If it is disabled, the access point is remotely deployed which increases the security risk.
PoE Status	Indicates the power over ethernet status of the access point. The possible values include: – Low—The access point draws low power from the ethernet. – Lower than 15.4 volts—The access point draws lower than 15.4 volts from the ethernet. – Lower than 16.8 volts—The access point draws lower than 16.8 volts from the ethernet. – Normal—The power is high enough for the operation of the access point. – Not Applicable—The power source is not from the ethernet.
Primary Controller	Indicates the name of the primary controller for this access point.
Radio MAC	Indicates the radio MAC address.
Reg. Domain Supported	Indicates whether or not the regulatory domain is supported.
Serial Number	Indicates the access point serial number.
Slot	Indicates the slot number.
Tx Power Control	Indicates whether the transmission power control is automatic or custom.
Tx Power Level	Indicates the transmission power level.
Up Time	Indicates how long the access point has been up in days, hours, minutes and seconds.
WLAN Override Names	Indicates the WLAN override profile names.
WLAN Override	Indicates whether WLAN Override is enabled or disabled.

Configuring the List of Access Points Display

The **Edit View** page allows you to add, remove, or reorder columns in the Access Points table.

To edit the available columns in the alarms table, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Click the **Edit View** link.

Step 3 To add an additional column to the access points table, click to highlight the column heading in the left column. Click **Show** to move the heading to the right column. All items in the right column are displayed in the table.

Step 4 To remove a column from the access points table, click to highlight the column heading in the right column. Click **Hide** to move the heading to the left column. All items in the left column are not displayed in the table.

Step 5 Use the **Up/Down** buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click **Up** or **Down** to move it higher or lower in the current list.

Step 6 Click **Reset** to restore the default view.

Step 7 Click **Submit** to confirm the changes.

Note See the "Viewing List of Access Points" section on page 5-43 for additional access point parameters than can be added through Edit View.

Generating a Report for Access Points

To generate a report for access points, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Click to select the access point(s) for which you want to run a report.

Step 3 Choose the applicable report from the Select a report drop-down list.

Step 4 Click **Go**.

The following reports are available:

Table 5-42 Access Point Reports

Report	Description	Reference
Load	Generates a report with load information.	Monitoring Traffic Load, page 5-48
Dynamic Power Control	Generates a report with Dynamic Power Control information.	Monitoring Dynamic Power Control, page 5-49
Noise	Generates a report with Noise information.	Monitoring Access Points Noise, page 5-50
Interference	Generates a report with Interference information.	Monitoring Access Points Interference, page 5-50
Coverage (RSSI)	Generates a report with Coverage (RSSI) information.	Monitoring Access Points Coverage (RSSI), page 5-51
Coverage (SNR)	Generates a report with Coverage (SNR) information.	Monitoring Access Points Coverage (SNR), page 5-51

Table 5-42 Access Point Reports

Report	Description	Reference
Up/Down Statistics	Time in days, hours and minutes since the last reboot. Generates a report with Up Time information.	Monitoring Access Points Up/Down Statistics, page 5-51
Voice Statistics	Generates a report for selected access points showing radio utilization by voice traffic.	Monitoring Access Points Voice Statistics, page 5-52
Voice TSM Table	Generates a report for selected access points and radio, organized by client device showing QoS status, PLR, and latency of its voice traffic stream.	Monitoring Access Points Voice TSM Table, page 5-52
Voice TSM Reports	Graphical representation of the TSM table except that metrics from the clients are averaged together on the graphs.	Monitoring Access Points Voice TSM Reports, page 5-54
802.11 Counters	Displays counters for access points at the MAC layer. Statistics such as error frames, fragment counts, RTS/CTS frame count, and retried frames are generated based on the filtering criteria and can help interpret performance (and problems, if any) at the MAC layer.	Monitoring Access Points 802.11 Counters, page 5-54
AP Profile Status	Displays access point load, noise, interference, and coverage profile status.	Monitoring Access Points AP Profile Status, page 5-55
Air Quality vs. Time	Displays the air quality index of the wireless network during the configured time duration.	Monitoring Air Quality, page 5-56
Traffic Stream Metrics	Useful in determining the current and historical quality of service (QoS) for given clients at the radio level. It also displays uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.	Monitoring Access Points Traffic Stream Metrics, page 5-55
Tx Power and Channel	Displays the channel plan assignment and transmit power level trends of devices based on the filtering criteria used when the report was generated. It could help identify unexpected behavior or issues with network performance.	Monitoring Access Points Tx Power and Channel, page 5-55

Table 5-42 Access Point Reports

Report	Description	Reference
VoIP Calls Graph	Helps analyze wireless network usage from a voice perspective by providing details such as the number and duration of VoIP calls (per radio) on the network over time. To be able to gather useful data from this report, VoIP snooping must be enabled on the WLAN. This report displays information in a graph.	Monitoring VoIP Calls, page 5-56
VoIP Calls Table	Provides the same information as the VoIP Calls Graph report but in table form.	Monitoring VoIP Calls, page 5-56
Voice Statistics	Helps analyze wireless network usage from a voice perspective by providing details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, and rejected calls (per radio) on the network. To be able to gather useful data from this report, make sure call admission control (CAC) is supported on voice clients.	Monitoring Voice Statistics, page 5-56
Worst Air Quality APs		Monitoring Air Quality, page 5-56

Monitoring Traffic Load

Traffic Load is the total amount of bandwidth used for transmitting and receiving traffic. This enables WLAN managers to track network growth and plan network growth ahead of client demand.

To access the access point load report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

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

Step 3 From the Generate a report for selected APs drop-down list, choose **Load**.

Step 4 Click **Go**. The Load report displays for the selected access points.

This page displays the following load data:

Table 5-43 Traffic Load

Parameter	Description
AP Name	Click the access point name to view access point details. See the "Monitoring Access Points Details" section on page 5-56 for more information.
Radio	Protocol of the rogue access point is either 802.11a, 802.11b or 802.11g. Click the radio to view On-Demand Statistics for this access point. See the "Monitoring Access Point Radio Details" section on page 5-68 for more information.
Attached Client Count	Number of clients attached (Actual and Threshold.)
Channel Utilization	802.11a RF utilization threshold between 0 and 100 percent (Actual and Threshold).
Receive Utilization	802.11a or 802.11b/g RF receive utilization threshold between 0 and 100 percent.
Transmit Utilization	802.11a or 802.11b/g RF transmit utilization threshold between 0 and 100 percent.
Status	Status of the client connection.

Monitoring Dynamic Power Control

To access the access point Load report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

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

Step 3 From the Generate a report for selected APs drop-down list, choose **Dynamic Power Control**.

Step 4 Click **Go**. The Dynamic Power Control report displays for the selected access points.

This page displays dynamic control parameters for access points as follows:

Table 5-44 Dynamic Power Control

Parameter	Description
AP Name	This is the name assigned to the access point. Click an access point name in the list to access its parameters. See the "Monitoring Access Points Details" section on page 5-56 for more information.
Radio	Protocol of the rogue access point is either 802.11a, or 802.11b/g. Click a Cisco Radio on the list to access its parameters. See the "Monitoring Access Point Radio Details" section on page 5-68 for more information.

Table 5-44 Dynamic Power Control

Parameter	Description
Current Power Level	Displays the operating transmit power level from the transmit power table. Access point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power. **Note** The power levels and available channels are defined by the Country Code Setting, and are regulated on a country by country basis.
Power Assignment Mode	Dynamic transmit power assignment has three modes: – Automatic—The transmit power will be periodically updated for all Cisco 1000 Series lightweight access points that permit this operation. – On Demand—Transmit power is updated when the Assign Now button is selected. – Fixed—No dynamic transmit power assignments occur and value are set to their global default. The default is Automatic. – Recommended Power Level.

Monitoring Access Points Noise

To access the access point Noise report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

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

Note If multiple access points are selected, they must have the same radio type.

Step 3 From the Generate a report for selected APs drop-down list, choose **Noise**.

Step 4 Click **Go**. The Noise report displays for the selected access points.

This page displays a bar graph of noise (RSSI in dBm) for each channel.

Monitoring Access Points Interference

To access the access point Interference report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

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

Note If multiple access points are selected, they must have the same radio type.

Step 3 From the Generate a report for selected APs drop-down list, choose **Interference**.

Step 4 Click **Go**. The Interference report displays for the selected access points.

This page displays a bar graph of interference (RSSI in dBm) for each channel:

- High interference -40 to 0 dBm.
- Marginal interference -100 to -40 dBm.
- Low interference -110 to -100 dBm.

Monitoring Access Points Coverage (RSSI)

To access the access point Coverage (RSSI) report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

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

Step 3 From the Generate a report for selected APs drop-down list, choose **Coverage (RSSI)**.

Step 4 Click **Go**. The Coverage (RSSI) report displays for the selected access points.

This page displays a bar graph of client distribution by received signal strength showing the number of clients versus RSSI in dBm.

Monitoring Access Points Coverage (SNR)

To access the access point Coverage (SNR) report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

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

Step 3 From the Generate a report for selected APs drop-down list, choose **Coverage (SNR)**.

Step 4 Click **Go**. The Coverage (SNR) report displays for the selected access points.

This page displays a bar graph of client distribution by signal-to-noise ratio showing the number of clients versus SNR.

Monitoring Access Points Up/Down Statistics

To access the access point Up/Down Statistics report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Select the check box of the applicable access point.

Step 3 From the Generate a report for selected APs drop-down list, choose **Up/Down Statistics**.

Click **Go**. The Up/Down Statistics report displays for the selected access points.

Note Up Time is time in days, hours, and minutes since the last reboot.

This page displays a line graph of access point up time graphed against time.

If you select more than one access point, the following message appears:

```
Please select only one AP for the Up Time Report.
```

Monitoring Access Points Voice Statistics

This generates a report for selected access points showing radio utilization by voice traffic. The report includes the number of current calls.

Note Voice Statistics reports are only applicable for CAC/WMM clients.

To access the access point Voice Statistics report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

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

Step 3 From the Generate a report for selected APs drop-down list, choose **Voice Statistics**.

Click **Go**. The Voice Statistics report displays for the selected access points.

The page displays the following access point voice statistics:

- AP Name—Select an item under AP Name. For more information, see the "Monitoring Access Points Details" section on page 5-56.
- Radio—Select an item under Radio. For more information, see the "Monitoring Access Point Radio Details" section on page 5-68.
- Calls in Progress—Number of calls in progress.
- Roaming Calls in Progress—Number of roaming calls in progress.
- Bandwidth in Use—Percentage of bandwidth in use.

Monitoring Access Points Voice TSM Table

This generates a report for selected access points and radio, organized by client device showing QoS status, PLR, and latency of its voice traffic stream.

To access the access point Voice TSM Table report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Select the check box of the applicable access point.

Step 3 From the Generate a report for selected APs drop-down list, choose **Voice TSM Table**.

Step 4 Click **Go**. The Voice TSM Table report displays for the selected access point.

The page displays the following voice TSM data:

Table 5-45 Voice TSM table

Parameter	Description
Time	Time that the statistics were gathered from the access point(s).
Client MAC	MAC address of the client. This shows a list of the clients evaluated during the most recent 90 second interval. The client could be a VoIP phone, laptop, PDA and refers to any client attached to the access point collecting measurements.
QoS	QoS values (packet latency, packet jitter, packet loss, roaming time) which can affect the WLAN are monitored. Access points and clients measure the metrics, access points collect the measurements and send them to the controller. The access points update the controller with traffic stream metric information every 90 seconds and 10 minutes of data is stored at one time.
% PLR (Downlink)	Percentage of packets lost on the downlink (access point to client) during the 90 second interval.
% PLR (Uplink)	Percentage of packets lost on the uplink (client to access point) during the 90 second interval.
Avg Queuing Delay (ms) (Downlink)	Average queuing delay in milliseconds for the downlink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.
Avg Queuing Delay (ms) (Uplink)	Average queuing delay in milliseconds for the uplink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.
% Packets > 40 ms Queuing Delay	Percentage of queuing delay packets greater than 40 ms.
% Packets > 20 ms Queuing Delay	Percentage of queuing delay packets greater than 20 ms.
Roaming Delay	Roaming delay in milliseconds. Roaming delay, which is measured by clients, is measured beginning when the last packet is received from the old access point and ending when the first packet is received from the new access point after a successful roam.

Monitoring Access Points Voice TSM Reports

This report provides a graphical representation of the TSM table except that metrics from the clients are averaged together on the graphs.

To access the access point Voice TSM report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Select the check box of the applicable access point.

Step 3 From the Generate a report for selected APs drop-down list, choose **Voice TSM Reports**.

Click **Go**. The Voice TSM Table report displays for the selected access point.

This page displays line graphs of the following downlink and uplink metric information, including times and dates:

Table 5-46 Voice TSM Reports

Parameter	Description
Average Queuing Delay (ms)	Average queuing delay in milliseconds. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.
% Packet with less than 10 ms delay	Percentage of packets with less than 10 milliseconds delay.
% Packet with more than 10 < 20 ms delay	Percentage of packets with more than 10 milliseconds delay but less than 20 milliseconds delay.
% Packet with more than 20 < 40 ms delay	Percentage of packets with more than 20 milliseconds delay but less than 40 milliseconds delay.
% Packet with more than 40 ms delay	Percentage of packets with more than 40 milliseconds delay.
Packet Loss Ratio	Ratio of lost packets.
Total Packet Count	Number of total packets.
Roaming Count	Number of packets exchanged for roaming negotiations in this 90 seconds metrics page.
Roaming Delay	Roaming delay in milliseconds.

Monitoring Access Points 802.11 Counters

Displays counters for access points at the MAC layer. Statistics such as error frames, fragment counts, RTS/CTS frame count, and retried frames are generated based on the filtering criteria and can help interpret performance (and problems, if any) at the MAC layer.

See the "802.11 Counters" section on page 14-144 for more information on 802.11 Counters reports.

Monitoring Access Points AP Profile Status

Displays access point load, noise, interference, and coverage profile status.

See the "AP Profile Status" section on page 14-91 for more information on AP Profile Status reports.

Monitoring Access Points Radio Utilization

See the "Network Utilization" section on page 14-149 for more information on Radio Utilization reports.

Monitoring Access Points Traffic Stream Metrics

Useful in determining the current and historical quality of service (QoS) for given clients at the radio level. It also displays uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.

See the "Traffic Stream Metrics" section on page 14-151 for more information on Traffic Stream Metrics reports.

Monitoring Access Points Tx Power and Channel

See the "Tx Power and Channel" section on page 14-154 for more information on Tx Power and Channel reports.

The Current Tx Power Level setting controls the maximum conducted transmit power. The maximum available transmit power varies according to the configured channel, individual country regulation, and access point capability. See the *Product Guide* or data sheet at www.cisco.com for each specific model to determine the access point capability.

The Current Tx Power Level setting of 1 represents the maximum conducted power setting for the access point. Each subsequent power level (for example. 2, 3, 4, and so on.) represents approximately a 50% (or 3dBm) reduction in transmit power from the previous power level.

Note The actual power reduction may vary slightly for different models of access points.

Based on the configured antenna gain, the configured channel, and the configured power level, the actual transmit power at the access point can be reduced so that the specific country regulations are not exceeded.

Note Irrespective of whether you choose Global or Custom assignment method, the actual conducted transmit power at the access point is verified such that country specific regulations are not exceeded.

Command Buttons

- Save—Save the current settings.
- Audit—Discover the present status of this access point.

Monitoring VoIP Calls

VoIP calls reports helps analyze wireless network usage from a voice perspective by providing details such as the number and duration of VoIP calls (per radio) on the network over time. To be able to gather useful data from this report, VoIP snooping must be enabled on the WLAN. This report displays information in a graph.

Click VoIP Calls Graph from the Report Launch Pad to open the VoIP Calls Graph Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See VoIP Calls Graph, page 14-156 for more information.

Monitoring Voice Statistics

Voice Statistics report helps analyze wireless network usage from a voice perspective by providing details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, and rejected calls (per radio) on the network. To be able to gather useful data from this report, make sure call admission control (CAC) is supported on voice clients. See Voice Statistics, page 14-159 for more information.

Monitoring Air Quality

To facilitate an "at a glance" understanding of where interference problems are impacting the network, it rolls up the detailed information into a high-level, easy-to- understand metric referred to as Air Quality (AQ). AQ is reported at a channel, floor, and system level and it supports AQ alerts, so that you can be automatically notified when AQ falls below a desired threshold. See Monitoring CleanAir Air Quality Events, page 5-147 for more information.

Monitoring Access Points Details

Access Points Details page enables you to view access point information for a single AP.

Choose **Monitor > Access Points** and click a list item under AP Name to access this page. Depending on the type of access point, the following tabs may be displayed. This section provides the detailed information regarding each Access Points Details page tab and contains the following topics:

- General Tab, page 5-56
- Interfaces Tab, page 5-64
- CDP Neighbors Tab, page 5-66
- Current Associated Clients Tab, page 5-66
- SSID Tab, page 5-67

General Tab

Note The General tab parameters differ between lightweight and autonomous access points.

- General Parameters—Lightweight Access Points
- General Parameters—Autonomous

General Parameters—Lightweight Access Points

Table 5-47 General- LightWeight Access Points

Parameter	Description
General	
AP Name	Operator defined name of access point.
AP IP address, Ethernet MAC address, and Base Radio MAC address	IP address, Ethernet MAC address and Radio MAC address.
Country Code	The codes of the supported countries. Up to 20 countries can be supported per controller. **Note** Access points may not operate properly if they are not designed for use in your country of operation. For a complete list of country codes supported per product, refer to http://www.cisco.com/en/US/docs/wireless/wcs/4.0/configuration/guide/wcscod.html.
Link Latency Settings	You can configure link latency on the controller to measure the link between an access point and the controller. See the "Configuring Link Latency Settings for Access Points" section on page 9-203 for more information. – Current Link Latency (in msec)—The current round-trip time (in milliseconds) of heartbeat packets from the access point to the controller and back. – Minimum Link Latency (in msec)—Because link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of heartbeat packets from the access point to the controller and back. – Maximum Link Latency (in msec)—Because link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of heartbeat packets from the access point to the controller and back.
LWAPP/CAPWAP Uptime	Displays how long the LWAPP/CAPWAP connection has been active.
LWAPP?CAPWAP Join Taken Time	Displays how long the LWAPP/CAPWAP connection has been joined.
Admin Status	The administration state of the access point as either enabled or disabled.
AP Mode	

Table 5-47 General- LightWeight Access Points

Parameter	Description
Local	Default mode. Data clients are serviced while configured channels are scanned for noise and rogues. The access point goes off-channel for 50 ms and listens for rogues. It cycles through each channel for the period specified under the Auto RF configuration. **Note** To configure Local or H-REAP access points for Cisco Adaptive wIPS feature, choose Local or H-REAP and select the **Enhanced wIPS Engine Enabled** check box.
Monitor	Radio receive only mode. The access point scans all configured channels every 12 seconds. Only deauthenticated packets are sent in the air with an access point configured this way. A monitor mode access point detects rogues, but it cannot connect to a suspicious rogue as a client to prepare for the sending of RLDP packets. **Note** To configure access points for Cisco Adaptive wIPS feature, select **Monitor**. Select the **Enhanced wIPS Engine Enabled** check box and choose **wIPS** from the Monitor Mode Optimization drop-down list. Before you can enable an access point to be in wIPS mode, you must disable the access point radios. If you do not disable the access point radio, an error message displays. **Note** Once you have enabled the access point for wIPS, re-enable the radios.
Rogue Detector	The access point radio is turned off and the access point listens to wired traffic only. The controllers that operate in this mode monitor the rogue access points. The controller sends all the rogue access point and client MAC address lists to the rogue detector, and the rogue detector forwards this information to the WLC. The MAC address list is compared to what the WLC access points heard over the network. If the MAC addresses match, you can determine which rogue access points are connected on the wired network.

Table 5-47 General- LightWeight Access Points

Parameter	Description
Sniffer	The access point captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. These packets contain information such as timestamp, signal strength, packet size, and so on. This feature can only be enabled if you run AiroPeek, which is a third-party network analyzer software that supports the decoding of data packets. For more information on AiroPeek, see www.wildpackets.com.
H-REAP	Enables hybrid REAP for up to six access points. The H-REAP access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. **Note** H-REAP must be selected to configure an OfficeExtend access point. When the AP mode is H-REAP, H-REAP configuration options display including the option to enable OfficeExtend AP and to enable Least Latency Controller Join.
Bridge	This is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The bridge and its wired clients are listed as client in NCS if the AP mode is set to Bridge, and the access point is bridge capable.
Spectrum Expert	This mode allows a CleanAir-enabled access point to be used extensively for interference detection on all monitored channels. All other functions such as IDS scanning and Wi-Fi are suspended.
Enhanced wIPs Engine	Enabled or Disabled, to enable the monitoring of the security attacks using Cisco Adaptive wIPS feature.
Operational Status	Registered or Not Registered, as determined by the controller.
Registered Controller	The controller to which the access point is registered. Click to display the registered controller details. See the "Monitoring System Summary" section on page 5-4 for more information.
Primary Controller	The name of the primary controller for this access point.

Table 5-47 General- LightWeight Access Points

Parameter	Description
Port Number	The SNMP name of the access point primary controller. The access point attempts to associate with this controller first for all network operations and in the event of a hardware reset.
AP Uptime	Displays how long the access point has been active to receive and transmit.
Map Location	Customer-definable location name for the access point. Click to look at the actual location on a map. See **Monitor** > **Access Points** > *name* > **Map Location** for more information.
Google Earth Location	Indicates whether a Google Earth location is assigned.
Location	The physical location where the access point is placed (or Unassigned).
Statistics Timer	This counter sets the time in seconds that the access point sends its DOT11 statistics to the controller.
PoE Status	The power over ethernet status of the access point. The possible values include: – Low—The access point draws low power from the Ethernet. – Lower than 15.4 volts—The access point draws lower than 15.4 volts from the Ethernet. – Lower than 16.8 volts—The access point draws lower than 16.8 volts from the Ethernet. – Normal—The power is high enough for the operation of the access point. – Not Applicable—The power source is not from the Ethernet.
Rogue Detection	Indicates whether or not Rogue Detection is enabled. See the “” section on page 5-152 for more information on rogue detection. **Note** Rogue detection is disabled automatically for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. For more information regarding OfficeExtend access points, see the *Cisco Wireless LAN Controller Configuration Guide*.

Table 5-47 General- LightWeight Access Points

Parameter	Description
OfficeExtend AP	Indicates whether or not the access point is enabled as an OfficeExtend access point. The default is Enabled.
Encryption	Indicates whether or not encryption is enabled. **Note** Enabling or disabling encryption functionality causes the access point to reboot which then causes a loss of connectivity for clients. **Note** DTLS data encryption is enabled automatically for OfficeExtend access points to maintain security. Encryption is only available if the access point is connected to a 5500 series controller with a Plus license.
Least Latency Join	The access point switches from a priority order search (primary, secondary, and then tertiary controller) to a search for the controller with the best latency measurement (least latency). The controller with the least latency provides the best performance.
Telnet Access	Indicates whether or not Telnet Access is enabled.
SSH Access	Indicates whether or not SSH is enabled. **Note** An OfficeExtend access point may be connected directly to the WAN which could allow external access if the default password is used by the access point. Because of this, Telnet and SSH access are disabled automatically for OfficeExtend access points.
Versions	
Software Version	The operating system release.version.dot.maintenance number of the code currently running on the controller.
Boot Version	The operating system bootloader version number.
Inventory Information	
AP Type	Type of Access Point
AP Model	Access point model number.
Cisco IOS Version	The Cisco IOS version details
AP Certificate Type	Either Self Signed or Manufacture Installed.
H-REAP Mode Supported	Indicates if H-REAP mode is supported or not.
wIPS Profile (when applicable)	

Table 5-47 General- LightWeight Access Points

Parameter	Description
Profile Name	Click the user-assigned profile name to view wIPS profile details.
Profile Version	
Unique Device Identifier (UDI)	
Name	Name of Cisco AP for access points.
Description	Description of access point.
Product ID	Orderable product identifier.
Version ID	Version of product identifier.
Serial Number	Unique product serial number.
Run Ping Test Link	Click to ping the access point. The results are displayed in a pop-up dialog box.
Alarms Link	Click to display alarms associated with this access point.
Events Link	Click to display events associated with this access point.

General Parameters—Autonomous

Note For autonomous clients, NCS *only* collects client counts. The client counts in the Monitor page and reports have autonomous clients included. Client search, client traffic graphs, or other client reports (such as Unique Clients, Busiest Clients, Client Association) do *not* include clients from autonomous access points.

Table 5-48 General Parameters - Autonomous

Parameters	Description
AP Name	Operator defined name of access point.
AP IP address and Ethernet MAC address	IP address, Ethernet MAC address of the access point.
AP UpTime	Indicates how long the access point has been up in number of days, hours, minutes, and seconds.
Map Location	Customer-definable location name for the access point. Click to look at the actual location on a map. See the“Monitoring Maps” section on page 6-8 for more information.
WGB Mode	Indicates whether or not the access point is in work group bridge mode.
SNMP Info	

Table 5-48 General Parameters - Autonomous

Parameters	Description
SysObjectId	System Object ID.
SysDescription	The system device type and current version of firmware.
SysLocation	The physical location of the device, such as a building name or room in which it is installed.
SysContact	The name of the system administrator responsible for the device.
Versions	
Software Version	The operating system release.version.dot.maintenance number of the code currently running on the controller.
CPU Utilization	Displays the maximum, average, and minimum CPU utilization over the specified amount of time.
Memory Utilization	Displays the maximum, average, and minimum memory utilization over the specified amount of time.
Inventory Information	
AP Type	Autonomous or lightweight.
AP Model	The Access Point model number.
AP Serial Number	Unique serial number for this access point.
H-REAP Mode Supported	If H-REAP mode is supported or not.
Unique Device Identifier (UDI)	
Name	Name of Cisco AP for access points.
Description	Description of access point.
Product ID	Orderable product identifier.
Version ID	Version of product identifier.
Serial Number	Unique product serial number.

Note Memory and CPU utilization charts are displayed.

Note Click **Alarms** to display the alarms associated with the access point.
Click **Events** to display events associated with the access point.

Interfaces Tab

The Interfaces tab displays the following parameters:

Table 5-49 Interfaces Tab

Parameter	Description
Interface	
Admin Status	Indicates whether the Ethernet interface is enabled.
Operational Status	Indicates whether the Ethernet interface is operational.
Rx Unicast Packets	Indicates the number of unicast packets received.
Tx Unicast Packets	Indicates the number of unicast packets sent.
Rx Non-Unicast Packets	Indicates the number of non-unicast packets received.
Tx Non-Unicast Packets	Indicates the number of non-unicast packets sent.
Radio Interface	
Protocol	802.11a/n or 802.11b/g/n.
Admin Status	Indicates whether the access point is enabled or disabled.
CleanAir Capable	Indicates whether the access point is able to use CleanAir.
CleanAir Status	Indicates the status of CleanAir.
Channel Number	Indicates the channel on which the Cisco Radio is broadcasting.
Extension Channel	Indicates the secondary channel on which Cisco radio is broadcasting.
Power Level	Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.
Channel Width	Indicates the channel bandwidth for this radio interface. See the "Configuring 802.11a/n RRM Dynamic Channel Allocation" section on page 9-121 for more information on configuring channel bandwidth. Minimum (default) setting is 20 MHz. Maximum setting is the maximum channel width supported by this radio.
Antenna Name	Identifies the type of antenna.

Click an interface name to view its properties:

Table 5-50 Interface properties

Parameter	Description
AP Name	Name of the Access Point.
Link speed	Indicates the speed of the interface in Mbps.
RX Bytes	Indicates the total number of bytes in the error-free packets received on the interface.
RX Unicast Packets	Indicates the total number of unicast packets received on the interface.
RX Non-Unicast Packets	Indicates the total number of non-unicast or mulitcast packets received on the interface.

Table 5-50 Interface properties

Parameter	Description
Input CRC	Indicates the total number of CRC error in packets received on the interface.
Input Errors	Indicates the sum of all errors in the packets while receiving on the interface.
Input Overrun	Indicates the number of times the receiver hardware was incapable of handing received data to a hardware buffer because the input rate exceeded the receiver capability to handle the data.
Input Resource	Indicates the total number of resource errors in packets received on the interface.
Runts	Indicates the number of packets that are discarded because they are smaller than the medium minimum packet size.
Throttle	Indicates the total number of times the interface advised a sending NIC that it was overwhelmed by packets being sent and to slow the pace of delivery.
Output Collision	Indicates the total number of packet retransmitted due to an Ethernet collision.
Output Resource	Indicates the total number of resource errors in packets transmitted on the interface.
Output Errors	Indicates the sum of all errors that prevented the final transmission of packets out of the interface.
Operational Status	Indicates the operational state of the physical Ethernet interface on the AP.
Duplex	Indicates the duplex mode of an interface.
TX Bytes	Indicates the total number of bytes in the error-free packets transmitted on the interface.
TX Unicast Packets	Indicates the total number of unicast packets transmitted on the interface.
TX Non-Unicast Packets	Indicates the total number of non-unicast or mulitcast packets transmitted on the interface.
Input Aborts	Indicates the total number of packet aborted while receiving on the interface.
Input Frames	Indicates the total number of packet received incorrectly having a CRC error and a non-integer number of octets on the interface.
Input Drops	Indicates the total number of packets dropped while receiving on the interface because the queue was full.
Unknown Protocol	Indicates the total number of packet discarded on the interface due to an unknown protocol.
Giants	Indicates the number of packets that are discarded because they exceed the medium's maximum packet size.
Interface Resets	Indicates the number of times that an interface has been completely reset.

Table 5-50 Interface properties

Parameter	Description
Output No Buffer	Indicates the total number of packets discarded because there was no buffer space.
Output Underrun	Indicates the number of times the transmitter has been running faster than the router can handle.
Output Total Drops	Indicates the total number of packets dropped while transmitting from the interface because the queue was full.

CDP Neighbors Tab

The CDP Neighbors tab displays the following parameters:

Note This tab is visible only when the CDP is enabled.

Table 5-51 CDP Neighbors

Parameters	Description
AP Name	The name assigned to the access point.
AP IP Address	IP address of the access point.
Port No	Port number connected or assigned to the access point.
Local Interface	Identifies the local interface.
Neighbor Name	Name of the neighboring Cisco device.
Neighbor Address	Network address of the neighboring Cisco device.
Neighbor Port	Port of the neighboring Cisco device.
Duplex	Indicates Full Duplex or Half Duplex.
Interface Speed	Speed at which the interface operates.

Current Associated Clients Tab

The Current Associated Clients tab displays the following parameters:

Note This tab is visible only when there are clients associated to the AP (CAPWAP or Autonomous AP).

Table 5-52 Current Associated Clients

Parameter	Description
Username	Click the username to view the Monitor Client Details page for this client. See the "Monitoring Clients and Users" section on page 10-10 for more information.
IP Address	IP address of the associated client.

Table 5-52 Current Associated Clients

Parameter	Description
Client MAC Address	Click the client MAC address to view the Monitor Client Details page for this client. See the "Monitoring Clients and Users" section on page 10-10 for more information.
Association Time	Date and time of the association.
UpTime	Time duration of the association.
SSID	User-defined SSID name.
SNR (dB)	Signal to Noise Ratio in dB of the associated client.
RSSI	Received signal strength indicator in dBm.
Bytes Tx	This indicates the total amount of data that has passed through the ethernet interface either way.
Bytes Rx	This indicate the total amount of data that has been received through the ethernet interface either way
When the access point is not associated with the controller, then the database is used to retrieve the data (rather than the controller itself). If the access point is not associated, the following parameters appears:	
User Name	
IP Address	Local IP Address
Client MAC Address	Client MAC Address
Association Time	
Session Length	Time length of the session
SSID	User-defined SSID name.
Protocol	
Avg. Session Throughput	
Traffic (MB) as before	

Note Click the **Edit View** link to add, remove or reorder columns in the Current Associated Clients table. See the "Configuring the List of Access Points Display" section on page 5-45 for adding a new parameter using the Edit View.

SSID Tab

The SSID tab displays the following parameters:

Note This tab is visible only when the access point is Autonomous AP and there are SSID's configured on the AP.

Table 5-53 Current Associated Clients

Parameter	Description
SSID	Service Set Identifier being broadcast by the access point radio.
SSID Vlan	SSID on an access point is configured to recognize a specific VLAN ID or name.
SSID Vlan Name	SSID on an access point is configured to recognize a specific VLAN ID or name.
MB SSID Broadcast	SSID broadcast disabled essentially makes your Access Point invisible unless a wireless client already knows the SSID, or is using tools that monitor or 'sniff' traffic from an AP's associated clients.
MB SSID Time Period	Within this specified time period, internal communication within the SSID continues to work.

Monitoring Access Point Radio Details

Choose **Monitor > Access Points** and click a list item under Radio to access this page.

Choose **Monitor > Maps**, then click an item in the Name column, then click an access point icon to access this page.

Choose **Monitor > Access Points** and click a list item under AP Name, click 802.11a or 802.11b under AP Interfaces to access this page. This page enables you to view access point information for a single 802.11a or 802.11b/g Cisco Radio.

The default is to show On Demand Statistics. Use the View drop-down list to select a different view:

- Choose On Demand Statistics, and click **Go** to display "Monitoring On Demand Statistics".
- Choose Operational Parameters, and click **Go** to display "Monitoring Operational Parameters".
- Choose 802.11 MAC Counters, and click **Go** to display "Monitoring 802.11 MAC Counters".
- Choose View Alarms and, click **Go** to display "Monitoring View Alarms".
- Choose View Events and, click **Go** to display "Monitor View Events".

Monitoring On Demand Statistics

To view On Demand Statistics for an access point, click the Radio of the applicable access point from the Monitor > Access Points page. The Radio Details page defaults to On Demand Statistics. See the "Monitoring Access Point Radio Details" section on page 5-68 for more information on radio details.

Note You can also select On Demand Statistics from the View drop-down list located on the Radio Details page.

This page enables you to view the following access point 802.11a or 802.11b Cisco Radio statistics for a single access point.

General

- AP Name—Click to view the access point details. See the "Monitoring Access Points Details" section on page 5-56 for more information.
- AP MAC Address
- Radio
- CleanAir Capable—Indicates if the access point is CleanAir Capable.
- AP in SE-Connect Mode—Yes or No. Indicates if the access point is connected in SE-Connect mode.
- CleanAir Enabled—Indicates if CleanAir is enabled on this access point.
- CleanAir Sensor Status—Indicates the operational status of the CleanAir censor (Up or Down).
- Admin Status—Enabled or disabled.
- Operational Status—Displays the operational status of the Cisco Radios (Up or Down).
- Controller—Click to display controller system details. See the "Monitoring System Summary" section on page 5-4 for more information.
- Channel—The channel upon which the Cisco Radio is broadcasting.
- Extension Channel—Indicates the secondary channel on which Cisco radio is broadcasting.
- Channel Width—Indicates the channel bandwidth for this radio interface. See the "Configuring 802.11a/n RRM Dynamic Channel Allocation" section on page 9-121 for more information on configuring channel bandwidth.
- Power Level—Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.

  The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis.
- Port—(1 to 24) Port to which the access point is connected.
- Map Location—Click to display the floor map showing the access point location.

Management Frame Protection

- Protection Capability—All Frames
- Validation Capability—All Frames
- MFP Version Supported—Management Frame Protection version supported and configured.

Profile Information

- Noise Profile—Notification sent when Noise Profile state changes between Success and Failure.

- Interference Profile—Notification sent when Interference Profile state changes between Success and Failure.
- Load Profile—Notification sent when Load Profile state changes between Success and Failure.
- Coverage Profile—Notification sent when Coverage Profile state changes between Success and Failure.

Note Click Success or Failure to view associated alarms.

Noise by Channel (dBm)

Graph showing channel and noise.

Interference by Channel (dBm%)

Graph showing the percentage of interference per channel.

Note Channel Utilization is a combination of Receive Power (RX) + Transmit Power (TX) + Interference. Interference—Access points report on the percentage of the medium taken up by interfering 802.11 transmissions (this can be from overlapping signals from foreign APs, as well as non-neighbors).

Note The channel list (as configured from the RRM page) is scanned completely using the “channel scan duration” parameter under monitor intervals. For example, if scanning all 11 channels in 2.4 GHz, and using the default duration (180 seconds), you get: 180/11 = 16.36 seconds approximately between each channel that is being scanned.

Load Statistics

- RX Utilization—802.11a or 802.11b/g RF receive utilization threshold between 0 and 100 percent.
- TX Utilization—802.11a or 802.11b/g RF transmit utilization threshold between 0 and 100 percent.
- Channel Utilization—802.11a RF utilization threshold between 0 and 100 percent (Subcolumns for Actual and Threshold).
- Attached Client Count—The number of clients attached.

General Tab

The General tab displays the following information:

% Client Count by RSSI

Graph with % and Received Signal Strength Indicator.

% Client Count by SNR

Graph with % and Signal-to-Noise Ratio.

Channel Utilization (% Busy)

Graph displaying the channel number on the x-axis and channel utilization on the y-axis.

Noise by Channel(dBm)

Graph displaying the channel on the x-axis and power in dBm on the y-axis.

Rx Neighbors

- Radio MAC Address
- AP Name—Click to view access point details.
- Map—Click to view the map.
- Mobility Group-Leader IP Address
- Neighbor Channel
- Channel Bandwidth
- RSSI (dBm)

Channel Utilization Statistics

- Time
- Picc—Percentage of time consumed by received frames from co-channel APs and clients.
- Pib—Percentage of time consumed by interference on the channel which cannot be correctly demodulated.

Note Picc and Pib values should give a good indication of the percentage of time the access point is busy because of co channel interference.

CleanAir Tab

The CleanAir tab provides the following information:

Air Quality

This graph displays the air quality index of the wireless network. A value of 100 indicates the air quality is best and a value of 1 indicates maximum interference.

Interference Power

This graph displays the interference power of the interfering devices on the channel number.

Non-WiFi Channel Utilization

This graph displays the non-WiFi channel utilization of the wireless network.

Active Interferers

This section displays the details of the active interferers on the wireless network. The following details are available:

- Interferer Name—The name of the interfering device.
- Affected Channels—The channel the interfering device is affecting.
- Detected Time—The time at which the interference was detected.
- Severity—The severity index of the interfering device.
- Duty Cycle(%)—The duty cycle (in percentage) of the interfering device.
- RSSI(dBm)—The Received Signal Strength Indicator of the interfering device.

View Drop-Down List

- Choose On Demand Statistics, and click **Go** to display On Demand Statistics for this access point radio. See the "Monitoring On Demand Statistics" section on page 5-68 for more information.
- Choose Operational Parameters, and click **Go** to display Operational parameters for this access point radio. See the "Monitoring Operational Parameters" section on page 5-72 for more information.
- Choose 802.11 MAC Counters, and click **Go** to display 802.11 MAC Counters for this access point radio. See the "Monitoring 802.11 MAC Counters" section on page 5-75 for more information.
- Choose View Alarms,and click **Go** to display alarms for this access point radio. See the "Monitoring View Alarms" section on page 5-76 for more information.
- Choose View Events, and click **Go** to display events for this access point radio. See the "Monitor View Events" section on page 5-77 for more information.

Monitoring Operational Parameters

To view Operational Parameters for an access point radio, follow these steps:

Step 1 Choose **Monitor** > **Access Points**, click the radio for the applicable access point.

Step 2 From the **View** drop-down list, choose Operational Parameters.

Step 3 Click **Go**.

This page enables you to view configuration information for a single 802.11a or 802.11b Cisco radio.

General

- AP Name—Click to view the access point details. See the "Monitoring Access Points Details" section on page 5-56 for more information.
- AP MAC Address
- Radio
- Admin Status—Enabled or disabled.
- Operational Status—Displays the operational status of the Cisco Radios (Up or Down).
- Controller—Click to display controller system details. See the "Monitoring System Summary" section on page 5-4 for more information.

- Channel—The channel upon which the Cisco Radio is broadcasting.
- Extension Channel—Indicates the secondary channel on which Cisco radio is broadcasting.
- Channel Width—Indicates the channel bandwidth for this radio interface. See the "Configuring 802.11a/n RRM Dynamic Channel Allocation" section on page 9-121 for more information on configuring channel bandwidth.
- Power Level—Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.

  The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis.
- Port—(1 to 24) Port to which the access point is connected.
- Map Location—Click to display the floor map showing the access point location.

Station Configuration Parameters

- Configuration Type—Automatic or Custom.
- Number of WLANs—1 (one) is the default.
- Medium Occupancy Limit—Indicates the maximum amount of time, in TU, that a point coordinator may control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.
- CFP Period—The number of DTIM intervals between the start of CFPs.
- CFP Max. Duration—The maximum duration of the CFP in TU that may be generated by the PCF.
- BSSID—MAC address of the access point.
- Beacon Period—The rate at which the SSID is broadcast by the access point, from 100 to 600 milliseconds.
- DTIM Period—The number of beacon intervals that shall elapse between transmission of Beacon frames containing a TIM element whose DTIM Count field is 0. This value is transmitted in the DTIM Period field of Beacon frames.
- Country String—Identifies the country in which the station is operating. The first two octets of this string are the two character country code.

Physical Channel Parameters

- Current Channel—Current operating frequency channel.
- Configuration—Locally customized or globally controlled.
- Current CCA Mode—CCA method in operation. Valid values:
  - Energy detect only (edonly) = 01.
  - Carrier sense only (csonly) = 02.
  - Carrier sense and energy detect (edandcs)= 04.
  - Carrier sense with timer (cswithtimer)= 08.
  - High rate carrier sense and energy detect (hrcsanded)=16.
- ED/TI Threshold—The Energy Detect and Threshold being used to detect a busy medium (frequency). CCA reports a busy medium upon detecting the RSSI above this threshold.

Physical Antenna Parameters

- Antenna Type—Internal or External.
- Diversity—Enabled via the internal antennas or via either Connector A or Connector B. (Enabled or Disabled).

RF Recommendation Parameters

- Channel—802.11a Low Band, Medium Band, and High Band; 802.11b/g.
- Tx Power Level—Zero (0) if Radio Resource Management (RRM) disabled, 1 - 5 if Radio Resource Management (RRM) is enabled.
- RTS/CTS Threshold—Zero (0) if Radio Resource Management (RRM) disabled, 1 - 5 if Radio Resource Management (RRM) is enabled.
- Fragmentation Threshold—Zero (0) if Radio Resource Management (RRM) is disabled.

MAC Operation Parameters

- Configuration Type—Automatic or Custom.
- RTS Threshold—This attribute indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed.

  An RTS/CTS handshake is performed at the beginning of any frame exchange sequence where the MPDU is a Data or Management type, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute to be larger than the maximum MSDU size turns off the RTS/CTS handshake for Data or Management type frames transmitted by this STA. Setting this attribute to zero turns on the RTS/CTS handshake for all frames of Data or Management type transmitted by this STA. The default value of this attribute shall be 2347.
- Short Retry Limit—The maximum number of transmission attempts of a frame, the length of which is less than or equal to dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value of this attribute is 7.
- Long Retry Limit—The maximum number of transmission attempts of a frame, the length of which is greater than dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value of this attribute shall be 4.
- Fragmentation Threshold—The current maximum size, in octets, of the MPDU that may be delivered to the PHY. An MSDU shall be broken into fragments if its size exceeds the value of this attribute after adding MAC headers and trailers. An MSDU or MMPDU shall be fragmented when the resulting frame has an individual address in the Address1 field, and the length of the frame is larger than this threshold. The default value for this attribute shall be the lesser of 2346 or the aMPDUMaxLength of the attached PHY and shall never exceed the lesser of 2346 or the aMPDUMaxLength of the attached PHY. The value of this attribute shall never be less than 256.
- Max Tx MSDU Lifetime—The elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU shall be terminated. The default value of this attribute is 512.
- Max Rx Lifetime—The MaxReceiveLifetime shall be the elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU shall be terminated. The default value is 512.

Tx Power

- # Supported Power Levels—Five or fewer power levels, depending on operator preference.
- Tx Power Level x—Access point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.

Note The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis.

- Tx Power Configuration—Globally controlled or customized for this access point (Custom or Global).
- Current Tx Power Level—Displays the operating transmit power level from the transmit power table.

Monitoring 802.11 MAC Counters

To view Operational Parameters for an access point radio, follow these steps:

Step 1 Choose **Monitor** > **Access Points**, click the radio for the applicable access point.

Step 2 From the **View** drop-down list, choose **802.11 MAC Counters**.

Step 3 Click **Go**.

This page enables you to view 802.11 MAC Counter information for a single 802.11a or 802.11b Cisco Radio.

General

- AP Name—Click to view the access point details. See the "Monitoring Access Points Details" section on page 5-56 for more information.
- AP MAC Address
- Radio
- Admin Status—Enabled or disabled.
- Operational Status—Displays the operational status of the Cisco Radios (Up or Down).
- Controller—Click to display controller system details. See the "Monitoring System Summary" section on page 5-4 for more information.
- Channel—The channel upon which the Cisco Radio is broadcasting.
- Extension Channel—Indicates the secondary channel on which Cisco radio is broadcasting.
- Channel Width—Indicates the channel bandwidth for this radio interface. See the "Configuring 802.11a/n RRM Dynamic Channel Allocation" section on page 9-121 for more information on configuring channel bandwidth.

Note Minimum (default) setting is 20 MHz. Maximum setting is the maximum channel width supported by this radio.

- Power Level—Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.

  The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis.
- Port—(1 to 24) Port to which the access point is connected.
- Map Location—Click to display the floor map showing the access point location.

RF Counters

- Tx Fragment Count—This counter is incremented for each successfully received MPDU Data or Management type.
- Multicast Tx Frame Count—This counter 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 implies having received an acknowledgment to all associated MPDUs.
- Tx Failed Count—This counter increments when an MSDU is successfully transmitted after one or more retransmissions.
- Retry Count—This counter increments when an MSDU is successfully transmitted after one or more retransmissions.
- Multiple Retry Count—This counter increments when an MSDU is successfully transmitted after more than one retransmission.
- Frame Duplicate Count—This counter increments when a frame is received that the Sequence Control field indicates is a duplicate.
- RTS Success Count—This counter increments when a CTS is received in response to an RTS.
- RTS Failure Count—This counter increments when a CTS is not received in response to an RTS.
- ACK Failure Count—This counter increments when an ACK is not received when expected.
- Rx Fragment Count—The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
- Multicast Rx Framed Count—This counter increments when a MSDU is received with the multicast bit set in the destination MAC address.
- FCS Error Count—This counter increments when an FCS error is detected in a received MPDU.
- Tx Frame Count—This counter increments for each successfully transmitted MSDU.
- WEP Undecryptable Count—This counter increments when a frame is received with the WEP subfield of the Frame Control field set to one and the WEP On value for the key mapped to the AT MAC address indicates that the frame should not have been encrypted or that frame is discarded due to the receiving STA not implementing the privacy option.

Monitoring View Alarms

To access the **View Alarms** page from the Monitor Access Points page, follow these steps:

Note When the AP is disassociated, in the Monitor > Access Points page, the radio status will have critical status. There will be only one alarm, **AP disassociated**. This is because radio alarms will be correlated to AP disassociated alarm.

Note When the controller goes down, the controller inventory dashlet shows the controller status as critical. But the radio inventory dashlet, will retain the last known status. In Monitor > Access Point page, the AP alarm status is shown as "Unknown".

Step 1 Choose **Monitor > Access Points**.

Step 2 Select the Radio Type in the Radio Type column of the applicable access point.

Step 3 From the **View** drop-down list, choose **View Alarms**.

Step 4 Click **Go**.

For more information on Viewing Alarms, see the "Monitoring Alarms" section on page 5-125.

Monitor View Events

To access the **View Events** page from the Monitor Access Points page, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Select the Radio Type in the Radio Type column of the applicable access point.

Step 3 From the **View** drop-down list, select **View Events**.

Step 4 Click **Go**.

For more information on viewing events, see the "Monitoring Events" section on page 5-142.

Monitoring Mesh Access Points

Mesh Health monitors the overall health of Cisco Aironet 1500 and 1520 series outdoor access points as well as Cisco Aironet 1130 and 1240 series indoor access points when configured as mesh access points, except as noted. Tracking this environmental information is particularly critical for access points that are deployed outdoors. The following factors are monitored:

- Temperature: Displays the internal temperature of the access point in Fahrenheit and Celsius (Cisco Aironet 1510 and 1520 outdoor access points only).
- Heater status: Displays the heater as on or off (Cisco Aironet 1510 and 1520 outdoor access points only)
- AP Up time: Displays how long the access point has been active to receive and transmit.
- LWAPP Join Taken Time: Displays how long it took to establish the LWAPP connection (excluding Cisco Aironet 1505 access points).

- LWAPP Up Time: Displays how long the LWAPP connection has been active (excluding Cisco Aironet 1505 access points).

Mesh Health information is displayed in the General Properties page for mesh access points.

To view the mesh health details for a specific mesh access point, follow these steps:

Step 1 Choose **Monitor > Access Points**. A listing of radios belonging to access points appears.

Note The radio status (not an access point status) is displayed when you choose Monitor > Access Points. The given status is updated frequently from traps and wireless status polling and takes several minutes to reflect actual radio status. The overall status of an access point can be found by viewing the access point on a map.

Note You can also use the New Search button to display the mesh access point summary. With the New Search option, you can further define the criteria of the access points that appear. Search criteria include AP Type, AP Mode, Radio Type, and 802.11n Support.

Step 2 Click the AP Name link to display details for that mesh access point. The General tab for that mesh access point appears.

Note You can also access the General tab for a mesh access point from a Cisco NCS map page. To display the page, double-click the mesh access point label. A tabbed page appears and displays the General tab for the selected access point.

To add, remove, or reorder columns in the table, click the **Edit View** link In the Monitor > Access Points page.

Mesh Statistics for an Access Point

Mesh Statistics are reported when a child mesh access point authenticates or associates with a parent mesh access point.

Security entries are removed and no longer displayed when the child mesh access point disassociates from the controller.

The following mesh security statistics are displayed for mesh access points:

- Bridging
- Queue
- Security

To view the mesh statistics for a specific mesh access point, follow these steps.

Step 1 Choose **Monitor > Access Points**. A listing of radios belonging to access points appears.

Note The radio status (not an access point status) is displayed when you choose Monitor > Access Points. The given status is updated frequently from traps and wireless status polling and takes several minutes to reflect actual radio status. The overall status of an access point can be found by viewing the access point on a map.

Note You can also use the New Search button to display the access point summary. With the New Search option, you can further define the criteria of the access points that display. Search criteria include AP Name, IP address, MAC address, Controller IP or Name, Radio type, and Outdoor area.

Step 2 Click the **AP Name** link of the target mesh access point.

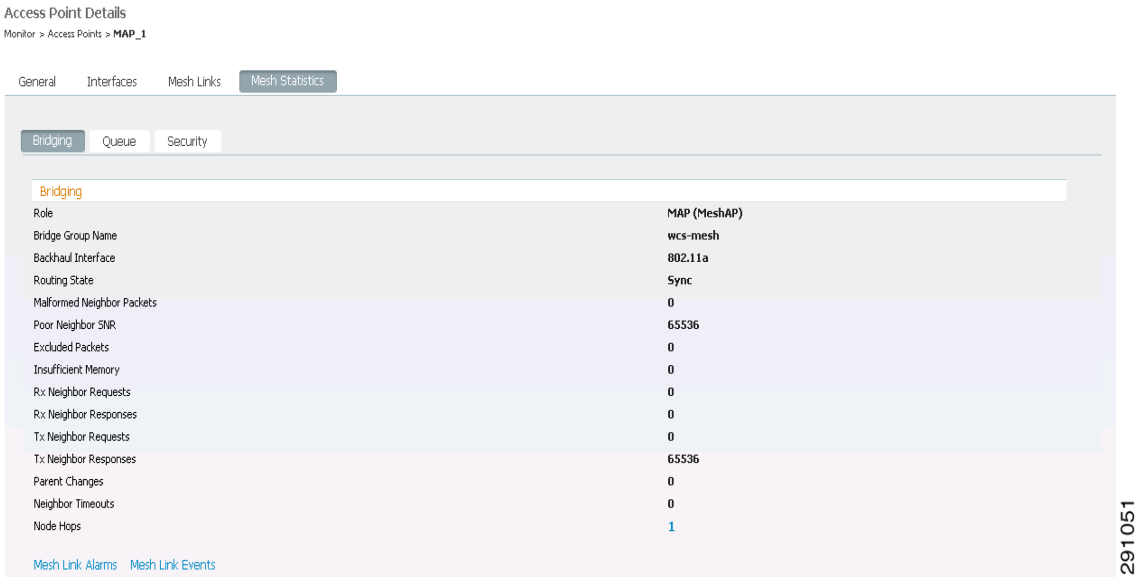
A tabbed page appears and displays the General Properties page for the selected access point.

Step 3 Click the **Mesh Statistics** tab (see Figure 5-1). A three-tabbed Mesh Statistics page appears.

Note The Mesh Statistics tab and its subordinate tabs (Bridging, Queue and Security) only appear for mesh access points. The Mesh Link Alarms and Mesh Link Events links are accessible from each of the three tabbed panels.

Note You can also access the Mesh Securities page for a mesh access point from a Cisco NCS map. To display the page, double-click the mesh access point label.

Figure 5-1 Monitor > Access Points > AP Name > Mesh Statistics



Bridging	
Role	MAP (MeshAP)
Bridge Group Name	wcs-mesh
Backhaul Interface	802.11a
Routing State	Sync
Malformed Neighbor Packets	0
Poor Neighbor SNR	65536
Excluded Packets	0
Insufficient Memory	0
Rx Neighbor Requests	0
Rx Neighbor Responses	0
Tx Neighbor Requests	0
Tx Neighbor Responses	65536
Parent Changes	0
Neighbor Timeouts	0
Node Hops	1

Summaries of the Bridging, Queue and Security Statistics and their definitions are provided in Table 5-54, Table 5-55 and Table 5-56 respectively.

Table 5-54 Bridging Mesh Statistics

Parameter	Description
Role	The role of the mesh access point. Options are mesh access point (MAP) and root access point (RAP).
Bridge Group Name	The name of the bridge group to which the MAP or RAP is a member. We recommend assigning membership in a bridge group name. If one is not assigned, a MAP is by default assigned to a default bridge group name.
Backhaul Interface	The radio backhaul for the mesh access point.
Routing State	The state of parent selection. Values that display are seek, scan and maint. Maint appears when parent selection is complete.
Malformed Neighbor Packets	The number of malformed packets received from the neighbor. Examples of malformed packets include malicious floods of traffic such as malformed or short DNS packets and malformed DNS replies.
Poor Neighbor SNR	The number of times the signal-to-noise ratio falls below 12 dB on the backhaul link.
Excluded Packets	The number of packets received from excluded neighbor mesh access points.
Insufficient Memory	The number of insufficient memory conditions.
RX Neighbor Requests	The number of broadcast and unicast requests received from the neighbor mesh access points.
RX Neighbor Responses	The number of responses received from the neighbor mesh access points.
TX Neighbor Requests	The number of unicast and broadcast requests sent to the neighbor mesh access points.
TX Neighbor Responses	The number of responses sent to the neighbor mesh access points.
Parent Changes	The number of times a mesh access point (child) moves to another parent.
Neighbor Timeouts	The number of neighbor timeouts.
Node Hops	The number of hops between the MAP and the RAP. Click the value link to display a dialog box which enables you to configure details of what is reported, how often the node hop value is updated, and view a graphical representation of the report.

Table 5-55 Queue Mesh Statistics

Parameter	Description
Silver Queue	The average and peak number of packets waiting in the silver (best effort) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.
Gold Queue	The average and peak number of packets waiting in the gold (video) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.
Platinum Queue	The average and peak number of packets waiting in the platinum (voice) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.
Bronze Queue	The average and peak number of packets waiting in the bronze (background) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.
Management Queue	The average and peak number of packets waiting in the management queue during the defined statistics time interval. Packets dropped and queue size is also summarized.

Table 5-56 Security Mesh Statistics

Parameter	Description
Packets Transmitted	Summarizes the total number of packets transmitted during security negotiations by the selected mesh access point.
Packets Received	Summarizes the total number of packets received during security negotiations by the selected mesh access point.
Association Request Failures	Summarizes the total number of association request failures that occur between the selected mesh access point and its parent.
Association Request Timeouts	Summarizes the total number of association request time outs that occur between the selected mesh access point and its parent.
Association Request Success	Summaries the total number of successful association requests that occur between the selected mesh access point and its parent.
Authentication Request Failures	Summarizes the total number of failed authentication requests that occur between the selected mesh access point and its parent.

Table 5-56 Security Mesh Statistics (continued)

Parameter	Description
Authentication Request Timeouts	Summarizes the total number of authentication request timeouts that occur between the selected mesh access point and its parent.
Authentication Request Success	Summarizes the total number of successful authentication requests between the selected mesh access point and its parent mesh node.
Reassociation Request Failures	Summarizes the total number of failed reassociation requests between the selected mesh access point and its parent.
Reassociation Request Timeouts	Summarizes the total number of reassociation request timeouts between the selected mesh access point and its parent.
Reassociation Request Success	Summarizes the total number of successful reassociation requests between the selected mesh access point and its parent.
Reauthentication Request Failures	Summarizes the total number of failed reauthentication requests between the selected mesh access point and its parent.
Reauthentication Request Timeouts	Summarizes the total number of reauthentication request timeouts that occurred between the selected mesh access point and its parent.
Reauthentication Request Success	Summarizes the total number of successful reauthentication requests that occurred between the selected mesh access point and its parent.
Invalid Association Request	Summarizes the total number of invalid association requests received by the parent mesh access point from the selected child mesh access point. This state might occur when the selected child is a valid neighbor but is not in a state that allows association.
Unknown Association Requests	Summarizes the total number of unknown association requests received by the parent mesh access point from its child. The unknown association requests often occur when a child is an unknown neighbor mesh access point.
Invalid Reassociation Request	Summarizes the total number of invalid reassociation requests received by the parent mesh access point from a child. This might happen when a child is a valid neighbor but is not in a proper state for reassociation.
Unknown Reassociation Request	Summarizes the total number of unknown reassociation requests received by the parent mesh access point from a child. This might happen when a child mesh access point is an unknown neighbor.

Retrieving the Unique Device Identifier on Controllers and Access Points

The unique device identifier (UDI) standard uniquely identifies products across all Cisco hardware product families, enabling customers to identify and track Cisco products throughout their business and network operations and to automate their asset management systems. The standard is consistent across all electronic, physical, and standard business communications. The UDI consists of five data elements:

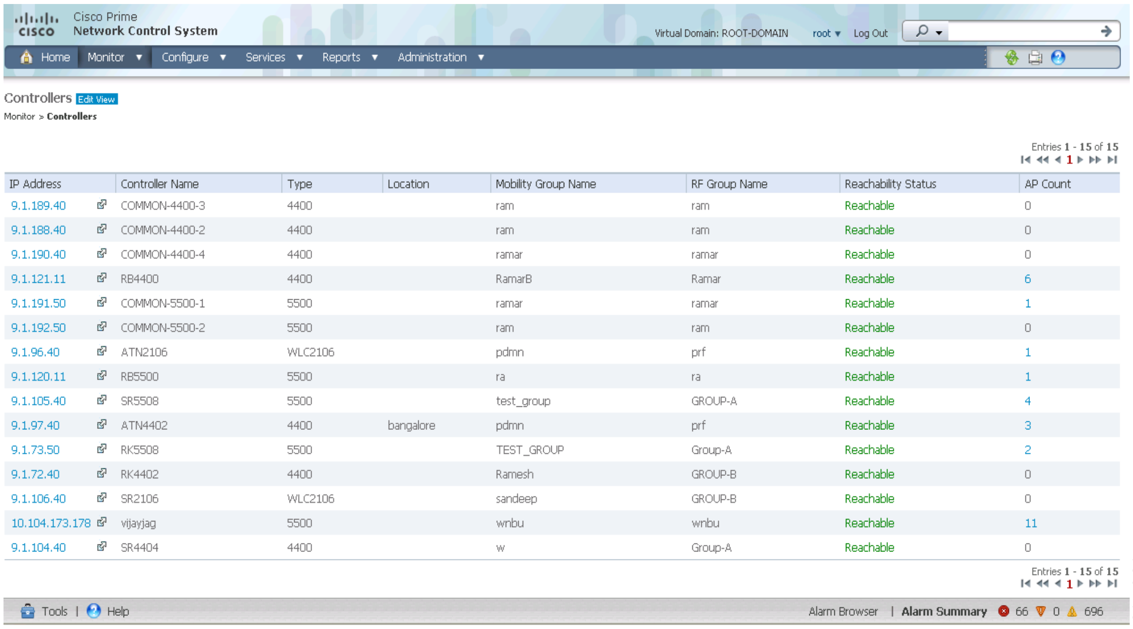
- The orderable product identifier (PID)
- The version of the product identifier (VID)
- The serial number (SN)
- The entity name
- The product description

The UDI is burned into the EEPROM of controllers and lightweight access points at the factory and can be retrieved through the GUI.

To retrieve the UDI on controllers and access points, perform the following steps:

Step 1 Choose **Monitor > Controllers/Access Points**. The Controllers/Access Points page appears (see Figure 5-2).

Figure 5-2 Monitor > Controllers Page



Controllers Edit View

Monitor > **Controllers**

Entries **1** - **15** of **15**

IP Address	Controller Name	Type	Location	Mobility Group Name	RF Group Name	Reachability Status	AP Count
9.1.189.40	COMMON-4400-3	4400		ram	ram	Reachable	0
9.1.188.40	COMMON-4400-2	4400		ram	ram	Reachable	0
9.1.190.40	COMMON-4400-4	4400		ramar	ramar	Reachable	0
9.1.121.11	RB4400	4400		RamarB	Ramar	Reachable	6
9.1.191.50	COMMON-5500-1	5500		ramar	ramar	Reachable	1
9.1.192.50	COMMON-5500-2	5500		ram	ram	Reachable	0
9.1.96.40	ATN2106	WLC2106		pdmn	prf	Reachable	1
9.1.120.11	RB5500	5500		ra	ra	Reachable	1
9.1.105.40	SR5508	5500		test_group	GROUP-A	Reachable	4
9.1.97.40	ATN4402	4400	bangalore	pdmn	prf	Reachable	3
9.1.73.50	RK5508	5500		TEST_GROUP	Group-A	Reachable	2
9.1.72.40	RK4402	4400		Ramesh	GROUP-B	Reachable	0
9.1.106.40	SR2106	WLC2106		sandeep	GROUP-B	Reachable	0
10.104.173.178	vijayjag	5500		wnbu	wnbu	Reachable	11
9.1.104.40	SR4404	4400		w	Group-A	Reachable	0

Entries **1** - **15** of **15**

Step 2 Click the IP address of the controller/access point (see in Figure 5-2) whose UDI information you want to retrieve. Data elements of the controller/access point UDI display. These elements are described in Table 5-57:.

Table 5-57 Maximum Number of Crypto Cards That Can Be Installed on a Cisco Wireless LAN Controller

Type of Controller	Maximum Number of Crypto Cards
Cisco 2000 Series	None

Table 5-57 Maximum Number of Crypto Cards That Can Be Installed on a Cisco Wireless LAN Controller

Type of Controller	Maximum Number of Crypto Cards
Cisco 4100 Series	One
Cisco 4400 Series	Two

Monitoring Coverage Hole

Coverage holes are areas where clients cannot receive a signal from the wireless network. The Cisco Unified Network Solution, radio resource management (RRM) identifies these coverage hole areas and reports them to the NCS, enabling the IT manager to fill holes based on user demand.

NCS is informed about the reliability-detected coverage holes by the controllers. NCS alerts the user about these coverage holes. For more information on finding coverage holes, refer to Cisco Context-Aware Services documentation at this location: http://www.cisco.com/en/US/docs/wireless/mse/3350/5.2/CAS/configuration/guide/msecg_ch7_CAS.html

Note Coverage holes are displayed as alarms. Pre-coverage holes are displayed as events.

Monitoring Pre-Coverage Holes

To view pre-coverage hole events, perform these steps:

Step 1 Choose **Monitor > Events** to display all current events.

Step 2 To view pre-coverage hole events only, click the **Advanced Search** link.

Step 3 In the New Search page, change the Search Category drop-down to **Events**.

Step 4 From the Event Category drop-down list, choose **Pre Coverage Hole**, and click **Go**.

The Pre-Coverage Hole Events page provides the information described in the following table (see Table 5-58):

Table 5-58 Pre-Coverage Hole Parameters

Parameter	Description
Severity	Pre-coverage hole events are always considered informational (Info).
Client MAC Address	MAC address of the client affected by the pre-coverage hole.
AP MAC Address	MAC address of the applicable access point.
AP Name	The name of the applicable access point.
Radio Type	The radio type (802.11b/g or 802.11a) of the applicable access point.
Power Level	Access point transmit power level: 1 = Maximum power allowed per country code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.

Table 5-58 Pre-Coverage Hole Parameters (continued)

Parameter	Description

Client Type	Client type can be any of the following:
	laptop(0)
	pc(1)
	pda(2)
	dot11mobilephone(3)
	dualmodephone(4)
	wgb(5)
	scanner(6)
	tabletpc(7)
	printer(8)
	projector(9)
	videoconfsystem(10)
	camera(11)
	gamingsystem(12)
	dot11deskphone(13)
	cashregister(14)
	radiotag(15)
	rfidsensor(16)
	server(17)

WLAN Coverage Hole Status	Determines if the current coverage hole state is enabled or disabled.
WLAN	The name for this WLAN.
Date/Time	The date and time the event occurred. Click the title to toggle between ascending and descending order.

Step 5 Choose a Client MAC Address to view pre-coverage hole details.

- General—Provides the following information:
  - Client MAC Address
  - AP MAC Address
  - AP Name
  - Radio Type
  - Power Level
  - Client Type
  - Category
  - Created
  - Generated By
  - Device AP Address

  - Severity
- Neighbor AP's—Indicates the MAC addresses of nearby access points, their RSSI values, and their radio types.
- Message—Describes what device reported the pre-coverage hole and on which controller it was detected.
- Help—Provides additional information, if available, for handling the event.

Monitoring Rogue Access Points

This section describes security solutions for rogue devices. A rogue device is an unknown access point or client that is detected by managed access points in your network.

Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain-text or other denial of service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as usernames and passwords. The hacker can then transmit a series of clear-to-send (CTS) frames. This action mimics an access point informing a particular client to transmit and instructing all others to wait, which results in legitimate clients being unable to access network resources. Therefore, wireless LAN service providers have a strong interest in banning rogue access points from the air space.

Because rogue access points are inexpensive and readily available, employees sometimes plug unauthorized rogue access points into existing LANs and build ad-hoc wireless networks without IT department knowledge or consent. These rogue access points can be a serious breach of network security as they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. Even more alarming, wireless users frequently publish insecure access point locations, increasing the odds of having enterprise security breached.

Detecting Rogue Devices

The controllers continuously monitor all nearby access points and automatically discover and collect information on rogue access points and clients. When a controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) to determine if the rogue is attached to your network.

Note NCS consolidates all of the controllers rogue access point data.

You can configure controllers to use RLDP on all access points or only on access points configured for monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded RF space, allowing monitoring without creating unnecessary interference and without affecting regular data access point functionality. If you configure a controller to use RLDP on all access points, the controller always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to either manually or automatically contain the detected rogue. See "Configuring Rogue Policies" for information on enabling RLDP.

Note Rogue access point partitions are associated with one of the detecting access points (the one with the latest or strongest RSSI value). If there is detecting access point information, NCS uses the detecting controller. If the rogue access point is detected by two controllers which are in different partitions, the rogue access point partition may be changed at any time.

This section contains the following topics:

- Viewing Rogue AP Alarm Details, page 5-94
- Monitoring Rogue AP Alarms, page 5-90
- Viewing Rogue AP Alarm Details, page 5-94
- Viewing Rogue Client Details, page 5-98
- Viewing Rogue AP History Details, page 5-99
- Viewing Rogue AP Event History Details, page 5-100
- Monitoring Adhoc Rogue Alarms, page 5-100

Classifying Rogue Access Points

Classification and reporting of rogue access points occurs through the use of rogue states and user-defined classification rules that enable rogues to automatically move between states. You can create rules that enable the controller to organize and display rogue access points as Friendly, Malicious, or Unclassified.

Note NCS consolidates all of the controllers rogue access point data.

By default, none of the classification rules are enabled. Therefore, all unknown access points are categorized as Unclassified. When you create a rule, configure conditions for it, and enable the rule, the unclassified access points are reclassified. Whenever you change a rule, it is applied to all access points (friendly, malicious, and unclassified) in the Alert state only.

Note Rule-based rogue classification does not apply to ad-hoc rogues and rogue clients.

Note The 5500 series controllers support up to 2000 rogues (including acknowledged rogues); the 4400 series controllers, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch support up to 625 rogues; and the 2100 series controllers and Controller Network Module for Integrated Services Routers support up to 125 rogues. Each controller limits the number of rogue containments to three per radio (or six per radio for access points in monitor mode).

When the controller receives a rogue report from one of its managed access points, it responds as follows:

1. The controller verifies that the unknown access point is in the friendly MAC address list. If it is, the controller classifies the access point as Friendly.
2. If the unknown access point is not in the friendly MAC address list, the controller starts applying rogue classification rules.

3. If the rogue is already classified as Malicious, Alert or Friendly, Internal or External, the controller does not reclassify it automatically. If the rogue is classified differently, the controller reclassifies it automatically only if the rogue is in the Alert state.
4. The controller applies the first rule based on priority. If the rogue access point matches the criteria specified by the rule, the controller classifies the rogue according to the classification type configured for the rule.
5. If the rogue access point does not match any of the configured rules, the controller classifies the rogue as Unclassified.
6. The controller repeats the previous steps for all rogue access points.
7. If RLDP determines that the rogue access point is on the network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if no rules are configured. You can then manually contain the rogue (unless you have configured RLDP to automatically contain the rogue), which would change the rogue state to Contained. If the rogue access point is not on the network, the controller marks the rogue state as Alert, and you can manually contain the rogue.
8. If desired, you can manually move the access point to a different classification type and rogue state.

As mentioned previously, the controller can automatically change the classification type and rogue state of an unknown access point based on user-defined rules, or you can manually move the unknown access point to a different classification type and rogue state. Table 5-59 shows the allowable classification types and rogue states from and to which an unknown access point can be configured.

Table 5-59 Allowable Classification Type and Rogue State Transitions

From	To
Friendly (Internal, External, Alert)	Malicious (Alert)
Friendly (Internal, External, Alert)	Unclassified (Alert)
Friendly (Alert)	Friendly (Internal, External)
Malicious (Alert, Threat)	Friendly (Internal, External)
Malicious (Contained, Contained Pending)	Malicious (Alert)
Unclassified (Alert, Threat)	Friendly (Internal, External)
Unclassified (Contained, Contained Pending)	Unclassified (Alert)
Unclassified (Alert)	Malicious (Alert)

If the rogue state is Contained, you have to uncontain the rogue access point before you can change the classification type. If you want to move a rogue access point from Malicious to Unclassified, you must delete the access point and allow the controller to reclassify it.

Rogue access points classification types include:

- Malicious—Detected but untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification. See “Malicious Rogue APs” for more information.
- Friendly—Known, acknowledged, or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained. See “Friendly Rogue APs” for more information. For more information on configuring friendly access point rules, see “Configuring a Friendly Access Point Template”.

- Unclassified—Rogue access point that are not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list. See for more information. See "Unclassified Rogue APs" for more information.

Malicious Rogue APs

Malicious rogue access points are detected but untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification.

The Security dashboard of the NCS home page displays the number of malicious rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active malicious rogue access points.

Malicious rogue access point states include:

- Alert—Indicates that the access point is not on the neighbor list or part of the user-configured Friendly AP list.
- Contained—The unknown access point is contained.
- Threat—The unknown access point is found to be on the network and poses a threat to WLAN security.
- Contained Pending—Indicates that the containment action is delayed due to unavailable resources.
- Removed—This unknown access point was seen earlier but is not seen now.

Click an underlined number in any of the time period categories for detailed information regarding the malicious rogue access points. See "Monitoring Rogue Access Points" for more information.

Friendly Rogue APs

Friendly rogue access points are known, acknowledged or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained.

Note Only NCS user can add a rogue access point MAC address to the Friendly AP list. The NCS will not apply the Friendly AP MAC address to controllers.

The Security dashboard of the NCS home page displays the number of friendly rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active friendly rogue access points.

Friendly rogue access point states include:

- Internal—If the unknown access point is inside the network and poses no threat to WLAN security, you would manually configure it as Friendly, Internal. For example, the access points in your lab network.
- External—If the unknown access point is outside the network and poses no threat to WLAN security, you would manually configure it as Friendly, External. For example, the access points belonging to a neighboring coffee shop.
- Alert—The unknown access point is not on the neighbor list or part of the user-configured Friendly AP list.

Click an underlined number in any of the time period categories for detailed information regarding the friendly rogue access points. See "Monitoring Rogue Access Points" for more information.

To delete a rogue access point from the Friendly AP list, ensure that both the NCS and controller remove the rogue access point from the Friendly AP list. Change the rogue access point from Friendly AP Internal or External to Unclassified or Malicious Alert.

Unclassified Rogue APs

An unclassified rogue access point refers to a rogue access point that is not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list.

The Security dashboard of the NCS home page displays the number of unclassified rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active unclassified rogue access points.

Unclassified rogue access point states include:

- 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 on the neighbor list or part of the user-configured Friendly AP list.
- Contained—The unknown access point is contained.
- Contained Pending—The unknown access point is marked Contained, but the action is delayed due to unavailable resources.

Click an underlined number in any of the time period categories for further information. See "Monitoring Rogue Access Points".

Monitoring Rogue AP Alarms

Rogue access point radios are unauthorized access points detected by one or more Cisco 1000 Series lightweight access points. To open the Rogue AP Alarms page, do one of the following:

- Search for rogue APs. See "Using the Search Feature" for more information about the search feature.
- From the NCS home page, click the Security dashboard. This page displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
- Click the **Malicious AP** number link in the Alarm Summary.

Note If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use it to view additional alarms.

Note Rogue access point partitions are associated with one of the detecting access points (the one with the latest or strongest RSSI value). If there is detecting access point information, NCS uses the detecting controller. If the rogue access point is detected by two controllers which are in different partitions, the rogue access point partition may be changed at any time.

The Rogue AP Alarms page contains the following parameters:

Note When NCS polls, some data may change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

- Severity—Indicates the severity of the alarm including:

Icon	Meaning
⊗	Critical
▼	Major
⚠	Minor
◆	Warning
ⓘ	Info
☑	Clear—Displays if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from NCS after 30 days.

You can use the Severity Configuration feature to determine the level of severity for the following rogue access point alarm types:

  - Rogue detected
  - Rogue detected contained
  - Rogue detected on network

See “Configuring Alarm Severities” for more information.

- Rogue MAC Address—Indicates the MAC address of the rogue access points. See “Viewing Rogue AP Alarm Details”.
- Vendor—Rogue access point vendor name or Unknown.
- Classification Type—Pending, Malicious, Friendly, or Unclassified.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Strongest AP RSSI—Displays the strongest AP RSSI for this rogue access point across the life of the rogue. The strongest AP RSSI over the life of the rogue displays to indicate the nearest distance that existed between the rogue access point and your building or location. The higher the RSSI, the closer the location.
- No. of Rogue Clients—Indicates the number of rogue clients associated to this rogue access point.

Note This number comes from the NCS database It is updated every two hours. From the **Monitor > Alarms > Alarm Details** page, this number is a real-time number. It is updated each time you open the Alarm Details page for this rogue access point.

- Owner—Name of person to which this alarm is assigned, or (blank).
- Last Seen Time—Indicates the date and time that the rogue access point was last seen.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point. See "Classifying Rogue Access Points" for additional information.
  - Malicious rogue states include: Alert, Contained, Threat, Contained Pending, and Removed. See "Malicious Rogue APs" for more information.
  - Friendly rogue states include: Internal, External, and Alert. See "Friendly Rogue APs" for more information.
  - Unclassified rogue states include: Pending, Alert, Contained, and Contained Pending. See "Unclassified Rogue APs" for more information.
- SSID—Indicates the service set identifier being broadcast by the rogue access point radio. It is blank if the SSID is not being broadcast.
- Map Location—Indicates the map location for this rogue access point.
- Acknowledged—Displays whether or not the alarm is acknowledged by the user.

  You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in NCS and you can search for all Acknowledged alarms using the alarm search functionality. See "Acknowledging Alarms" for more information.

  Note The alarm remains in NCS, and you can search for all Acknowledged alarms using the alarm search functionality.

Caution When you choose to contain a rogue device, the following warning appears: "There may be legal issues following this containment. Are you sure you want to continue?" The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another network could have legal consequences.

Select a command Menu

Select one or more alarms by selecting their respective check boxes, select one of the following commands from the Select a command drop-down list, and click **Go**.

- Assign to me—Assign the selected alarm(s) to the current user.
- Unassign—Unassign the selected alarm(s).
- Delete—Delete the selected alarm(s).
- Clear—Clear the selected alarm(s). Indicates that the alarm is no longer detected by any access point.

  Note Once the severity is Clear, the alarm is deleted from NCS after 30 days.

- Acknowledge Alarm—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See "Acknowledging Alarms" for more information.

  Note The alarm remains in NCS and you can search for all Acknowledged alarms using the alarm search functionality.

- Unacknowledge Alarm—Unacknowledge an already acknowledged alarm.
- Email Notification—Takes you to the All **Alarms** > **Email Notification** page to view and configure email notifications. See "Monitoring RFID Tags" for more information.
- Severity Configuration—Allows you to change the severity level for newly-generated alarms. See "Configuring Alarm Severities" for more information.
- Detecting APs—View the Cisco 1000 Series lightweight access points that are currently detecting the rogue access point. See "Detecting Access Points" for more information.
- Map (High Resolution)—Click to display a high-resolution map of the rogue access point location.
- Rogue Clients—Click to view a list of rogue clients associated with this rogue access point. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the Rogue access point. See "Viewing Rogue Client Details" for more information. This information can also be accessed by using the NCS Search feature. See "Using the Search Feature" or "Advanced Search" for more information.
- Set State to 'Unclassified - Alert'—Choose this command to tag the rogue access point as the lowest threat, continue monitoring the rogue access point, and to turn off Containment. See "Unclassified Rogue APs" for more information on Unclassified rogues.
- Set State to 'Malicious - Alert'—Choose this command to tag the rogue access point as 'Malicious'. See "Malicious Rogue APs" for more information on Malicious rogues.
- Set State to 'Friendly - Internal'—Choose this command to tag the rogue access point as internal, add it to the Known Rogue APs list, and to turn off Containment. See "Friendly Rogue APs" for more information on Friendly rogues.
- Set State to 'Friendly - External'—Choose this command to tag the rogue access point as external, add it to the Known Rogue APs list, and to turn off Containment. See "Friendly Rogue APs" for more information on Friendly rogues.
- 1 AP Containment—Target the rogue access point for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Target the rogue access point for containment by two Cisco 1000 Series lightweight access points.
- 3 AP Containment—Target the rogue access point for containment by three Cisco 1000 Series lightweight access points.
- 4 AP Containment—Target the rogue access point for containment by four Cisco 1000 Series lightweight access points. (Highest containment level.)

Note The higher the threat of the rogue access point, the higher the containment required.

Caution Attempting to contain a rogue access point may lead to legal consequences. When you select any of the AP Containment commands and click **Go**, a message `"Containing a Rogue AP may have legal consequences. Do you want to continue?"` appears. Click **OK** if you are sure or click **Cancel** if you do not wish to contain any access points.

Viewing Rogue AP Alarm Details

Rogue access point radios are unauthorized access points detected by Cisco 1000 Series lightweight access points. Alarm event details for each rogue access point are available from the Rogue AP Alarms list page.

To view alarm events for a rogue access point radio, click the rogue MAC address for the applicable alarm from the **Monitor** > **Alarms** page for rogue access point alarms.

Note All Alarm Details page fields (except No. of Rogue Clients) are populated through polling and are updated every two hours.
The number of rogue clients is a real-time number and is updated each time you access the Alarm Details page for a rogue access point alarm.

Note When NCS polls, some data may change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

The Alarm Details page displays the following information:

- General
  - Rogue MAC Address—MAC address of the rogue access points.
  - Vendor—Rogue access point vendor name or Unknown.

    Note When a rogue access point alarm displays for Airlink, the vendor displays as Alpha instead of Airlink.

  - Rogue Type—Indicates the rogue type such as AP.
  - On Network—Indicates how the rogue detection occurred.

    Controller—The controller detected the rogue (Yes or No).

    Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
  - Owner—Indicates the owner or is left blank.
  - Acknowledged—Indicates whether or not the alarm is acknowledged by the user.

    You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in NCS and you can search for all Acknowledged alarms using the alarm search functionality. See "Acknowledging Alarms" for more information.

- Classification Type—Malicious, Friendly, or Unclassified.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Channel Number—Indicates the channel of the rogue access point.
- Containment Level—Indicates the containment level of the rogue access point or Unassigned (not contained).
- Radio Type—Lists all radio types applicable to this rogue access point.
- Strongest AP RSSI—Displays the strongest AP RSSI for this rogue access point across the life of the rogue. The strongest AP RSSI over the life of the rogue displays to indicate the nearest distance that existed between the rogue access point and your building or location. The higher the RSSI, the closer the location.
- No. of Rogue Clients—Indicates the number of rogue clients associated to this rogue access point.

Note The number of rogue clients is the only real-time field in the **Monitor > Alarm > Alarm Details** page. It updates each time you open the Alarm Details page for this rogue access point.
All other fields on the Alarm Details page are populated through polling and are updated every two hours.

- First Seen Time—Indicates the date and time when the rogue access point was first detected. This information is populated from the controller.
- Last Seen Time—Indicates the date and time when the rogue access point was last detected. This information is populated from the controller.
- Modified—Indicates when the alarm event was modified.
- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).

  NMS (Network Management System - NCS)—Generated through polling. NCS periodically polls the controllers and generates events. NCS generates events when the traps are disabled or when the traps are lost for those events. In this case “Generated by” will be NMS.

  Trap—Generated by the controller. NCS process these traps and raises corresponding events for them. In this case “Generated by” will be Controller.
- Severity—The severity of the alarm including:

Icon	Meaning
⊗	Critical
▼	Major
⚠	Minor
◆	Warning

Icon	Meaning
ⓘ	Info
✓	Clear—Displays if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from NCS after 30 days.

You can use the Severity Configuration feature to determine the level of severity for rogue access points. See "Configuring Alarm Severities" for more information.

- Previous Severity—The previous severity of the alarm: Critical, Major, Minor, Clear.
- Event Details—Click the Event History link to view the event details.
- Rogue AP History—Click the Rogue AP History link to view the Rogue Alarm details.
- Switch Port Trace Status—Indicates the switch port trace status. Switch port trace status may include: Traced, but not found, Traced and found, Not traced, Failed. See "Configuring Switch Port Tracing" for more information.

- Switch Port Tracing Details—Provides the most recent switch port tracing details. To view additional trace details, use the **Click here for more details** link. See "Configuring Switch Port Tracing" for more information.
- Rogue Clients—Lists rogue clients for this access point including the client MAC address, the last date and time the client was heard, and the current client status. See "Viewing Rogue Client Details" for more information.

Note The number of rogue clients is the only real-time field on the **Monitor** > **Alarm** > **Alarm Details** page. It updates each time you open the Alarm Details page for this rogue access point.
All other fields on the Alarm Details page are populated through polling and are updated every two hours.

- Message—Displays the most recent message regarding this rogue access point. A message is sent for the following: When the rogue access point is first detected, for any trap sent, and for any changed state.
- Annotations—Lists current notes regarding this rogue access point. To add a new note, click **New Annotation**. Type the note and click **Post** to save and display the note or **Cancel** to close the page without saving the note.
- Location Notifications—Displays the number of location notifications logged against the client. Clicking a link displays the notifications.
- Location—Provides location information, if available.

Note The switch port tracing will not update any of the rogue attributes such as severity, state, and so on. As the rogue attributes are not updated by switch port tracing, alarms would not be triggered if a rogue is discovered to be 'on network' using switch port tracing.

Select a command Menu

The Select a command drop-down list located on the Rogue AP Alarm Details page provides the following options. Select an option from the drop-down list and click **Go**.

- Assign to me—Assign the selected alarm(s) to the current user.
- Unassign—Unassign the selected alarm(s).
- Delete—Delete the selected alarm(s).
- Clear—Clear the selected alarm(s).
- Acknowledge Alarm—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See "Acknowledging Alarms" for more information.

Note The alarm remains in NCS and you can search for all Acknowledged alarms using the alarm search functionality.

- Unacknowledge—Unacknowledge an already acknowledged alarm.
- Trace Switch Port—Click to run a switch port trace for this rogue access point. See "Configuring Switch Port Tracing" for more information.
- Event History—Click to view a list of events for this rogue access point. See "Monitoring Rogue Alarm Events" for more information.
- Refresh from Network—Click to sync up the rogue APs from the network.
- View Detecting AP on Network—View the Cisco 1000 Series lightweight access points that are currently detecting the rogue access point. See "Detecting Access Points" for more information.

Note Detecting AP Name, Radio, SSID information might be empty as the information is not available on controller. Refresh the page after the rogue AP task is completed to see the AP details.

- View Details by Controller—View the classification type and state of the rogue APs reported by the controller.
- Map (High Resolution)—Click to display a high-resolution map of the rogue access point location.
- Rogue Clients—Click to view a list of rogue clients associated with this rogue access point. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the Rogue access point. See "Viewing Rogue Client Details" for more information. This information can also be accessed by using the NCS Search feature. See "Using the Search Feature" or "Advanced Search" for more information.
- Set State to 'Unclassified - Alert'—Choose this command to tag the rogue access point as the lowest threat, continue monitoring the rogue access point, and to turn off Containment. See "Unclassified Rogue APs" for more information on Unclassified rogues.
- Set State to 'Malicious - Alert'—Choose this command to tag the rogue access point as 'Malicious'. See "Malicious Rogue APs" for more information on Malicious rogues.
- Set State to 'Friendly - Internal'—Choose this command to tag the rogue access point as internal, add it to the Known Rogue APs list, and to turn off Containment. See "Friendly Rogue APs" for more information on Friendly rogues.

- Set State to ‘Friendly - External’—Choose this command to tag the rogue access point as external, add it to the Known Rogue APs list, and to turn off Containment. See “Friendly Rogue APs” for more information on Friendly rogues.
- 1 AP Containment—Target the rogue access point for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Target the rogue access point for containment by two Cisco 1000 Series lightweight access points.
- 3 AP Containment—Target the rogue access point for containment by three Cisco 1000 Series lightweight access points.
- 4 AP Containment—Target the rogue access point for containment by four Cisco 1000 Series lightweight access points. (Highest containment level.)

Note The higher the threat of the rogue access point, the higher the containment required.

Viewing Rogue Client Details

You can view a list of rogue clients in several ways:

- Perform a search for rogue clients using the NCS Search feature. See the “Using the Search Feature” section on page 2-33 for more information.
- View the list of rogue clients for a specific rogue access point from the Alarm Details page for the applicable rogue access point.Click the Rogue MAC Address for the applicable rogue client to view the Rogue Client details page.
- From the Alarms Details page of a rogue access point, select **Rogue Clients** from the Select a command drop-down list.

The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the associated rogue access point.

Note Rogue client statuses include: Contained (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); and Threat (the rogue is a known threat).

Click the Client MAC Address for the rogue client to view the Rogue Client details page. The Rogue Client details page displays the following information:

- General—Information includes: client MAC address, number of access points that detected this client, when the client was first and last heard, the rogue access point MAC address, and the client current status.
- Location Notifications—Indicates the number of notifications for this rogue client including: absence, containment, distance, and all. Click the notification number to open the applicable **Monitor** > **Alarms** page.
- APs that detected the rogue client—Provides the following information for all access points that detected this rogue client: base radio MAC address, access point name, channel number, radio type, RSSI, SNR, and the date/time that the rogue client was last heard.
- Location—Provides location information, if available.

Note The higher the threat of the rogue access point, the higher the containment required.

Select a command

The Select a command drop-down list on the Rogue Client details page includes the following options:

- Set State to 'Unknown - Alert'—Choose this command to tag the rogue client as the lowest threat, continue monitoring the rogue client, and to turn off Containment.
- 1 AP Containment—Target the rogue client for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Target the rogue client for containment by two access points.
- 3 AP Containment—Target the rogue client for containment by three access points.
- 4 AP Containment—Target the rogue client for containment by four access points. (Highest containment level.)
- Map (High Resolution)—Click to display a high-resolution map of the rogue client location.
- Location History—Click to display the history of the rogue client location based on RF fingerprinting.

Viewing Rogue AP History Details

To view the history of a rogue AP alarms, click the Rogue AP History link in the Rogue AP Alarm page.

The Rogue AP History page displays the following information:

- Severity—The severity of the alarm.
- Rogue MAC Address—MAC address of the rogue access points.
- Classification Type—Malicious, Friendly, or Unclassified.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Strongest AP RSSI—Displays the strongest AP RSSI for this rogue access point across the life of the rogue. The strongest AP RSSI over the life of the rogue displays to indicate the nearest distance that existed between the rogue access point and your building or location. The higher the RSSI, the closer the location.
- No. of Rogue Clients—Indicates the number of rogue clients associated to this rogue access point.

Note The number of rogue clients is the only real-time field on the Monitor > Alarm > Alarm Details page. It updates each time you open the Alarm Details page for this rogue access point. All other fields on the Alarm Details page are populated through polling and are updated every two hours.

- First Seen Time—Indicates the date and time when the rogue access point was first detected. This information is populated from the controller.
- Last Seen Time—Indicates the date and time when the rogue access point was last detected. This information is populated from the controller.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point.

- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Category—Indicates the category of this alarm such as Security or NCS.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Channel Number—Indicates the channel of the adhoc rogue.
- Containment Level—Indicates the containment level of the adhoc rogue or Unassigned.
- Switch Port Trace Status—Indicates the switch port trace status. Switch port trace status may include: Traced, but not found, Traced and found, Not traced, Failed.

Click the Rogue MAC Address to view the specific rogue AP history details page. The rogue AP history details page displays the above details and also displays the actual alarm message.

Viewing Rogue AP Event History Details

To view the event details of a rogue AP, click the Event History link in the Rogue AP Alarm page.

The Rogue AP Event History page displays the following information:

- Severity—The severity of the alarm.
- Rogue MAC Address—MAC address of the rogue access points.
- Vendor—Rogue access point vendor name or Unknown.
- Classification Type—Malicious, Friendly, or Unclassified.
- On Network—Indicates whether the rogue detection occurred.The controller detected the rogue (Yes or No).
- Date/Time—The date and time that the event was generated.
- Radio Type—Lists all radio types applicable to this rogue access point.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

Monitoring Adhoc Rogues

If the MAC address of a mobile client operating in a adhoc network is not in the authorized MAC address list, then it is identified as an adhoc rogue.

- Monitoring Adhoc Rogue Alarms
- Viewing Adhoc Rogue Alarm Details

Monitoring Adhoc Rogue Alarms

The Adhoc Rogue Alarms page displays alarm events for adhoc rogues.To access the Adhoc Rogue Alarms page, do one of the following:

- Perform a search for adhoc rogue alarms. See "Using the Search Feature" for more information.
- From the NCS home page, click the Security dashboard. This page displays all the adhoc rogues detected in the past hour and the past 24 hours. Click the adhoc rogue number to view the adhoc rogue alarms.

If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

The Adhoc Rogue Alarms page contains the following parameters:

Note When NCS polls, some data may change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

- Severity—Indicates the severity of the alarm including:

Icon	Meaning
⊗	Critical
▼	Major
⚠	Minor
◆	Warning
ℹ	Info
☑	Clear—Displays if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from NCS after 30 days.

  You can use the Severity Configuration feature to determine the level of severity for the following adhoc rogue alarm types:

  - Adhoc Rogue auto contained
  - Adhoc Rogue detected
  - Adhoc Rogue detected on network
  - Adhoc Rogue detected on network

  See "Configuring Alarm Severities" for more information.

- Rogue MAC Address—Indicates the MAC address of the rogue. See "Viewing Adhoc Rogue Alarm Details" for more information.
- Vendor—Indicates the adhoc rogue vendor name, or Unknown.
- Radio Type—Lists all radio types applicable to this rogue access point.

- Strongest AP RSSI—Displays the strongest AP RSSI for this rogue across the life of the rogue. The strongest AP RSSI over the life of the rogue displays to indicate the nearest distance that existed between the rogue and your building or location. The higher the RSSI, the closer the location.

  No. of Rogue Clients—Indicates the number of rogue clients associated to this rogue access point.

  Note The number of rogue clients is the only real-time field on the **Monitor** > **Alarm** > **Alarm Details** page. It updates each time you open the Alarm Details page for this rogue access point.
  All other fields on the Alarm Details page are populated through polling and are updated every two hours.

- Owner—Indicates the owner or is left blank.
- Last Seen Time—Indicates the date and time that the alarm was last viewed.
- State—Indicates the state of the alarm. Possible states for adhoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
- SSID—The Service Set Identifier that is being broadcast by the rogue adhoc radio. It is blank if there is no broadcast.
- Map Location—Indicates the map location for this adhoc rogue.
- Acknowledged—Displays whether or not the alarm is acknowledged by the user.

  You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in NCS and you can search for all Acknowledged alarms using the alarm search functionality. See "Acknowledging Alarms" for more information.

Select a command Menu

Select one or more alarms by selecting their respective check boxes, select one of the following commands from the Select a command drop-down list, and click **Go**.

- Assign to me—Assign the selected alarm(s) to the current user.
- Unassign—Unassign the selected alarm(s).
- Delete—Delete the selected alarm(s).
- Clear—Clear the selected alarm(s).
- Acknowledge—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See "Acknowledging Alarms" for more information.

  Note The alarm remains in NCS and you can search for all Acknowledged alarms using the alarm search functionality.

- Unacknowledge—Unacknowledge an already acknowledged alarm.
- Email Notification—Takes you to the All **Alarms** > **Email Notification** page to view and configure email notifications. See "Monitoring RFID Tags" for more information.
- Detecting APs—View the access points that are currently detecting the rogue adhoc. See "Detecting Access Points" for more information.
- Map (High Resolution)—Click to display a high-resolution map of the adhoc rogue location.

- Rogue Clients—Click to view a list of rogue clients associated with this adhoc rogue. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the adhoc rogue.
- Set State to 'Alert'—Choose this command to tag the adhoc rogue as the lowest threat, continue monitoring the rogue access point, and to turn off Containment.
- Set State to 'Internal'—Choose this command to tag the adhoc rogue as internal, add it to the Known Rogue APs list, and to turn off Containment.
- Set State to 'External'—Choose this command to tag the adhoc rogue as external, add it to the Known Rogue APs list, and to turn off Containment.
- 1 AP Containment—Target the adhoc rogue for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Target the adhoc rogue for containment by two access points.
- 3 AP Containment—Target the adhoc rogue for containment by three access points.
- 4 AP Containment—Target the adhoc rogue for containment by four access points. (Highest containment level.)

Caution Attempting to contain an adhoc rogue may lead to legal consequences. When you select any of the AP Containment commands and click **Go**, a message "Containing a Rogue AP may have legal consequences. Do you want to continue?" appears. Click **OK** if you are sure, or click **Cancel** if you do not wish to contain any access points.

Viewing Adhoc Rogue Alarm Details

Alarm event details for each adhoc rogue are available from the Adhoc Rogue Alarms page.

To view alarm events for a adhoc rogue radio, click the applicable Rogue MAC Address from the Adhoc Rogue Alarms page.

This page displays alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by Cisco 1000 Series lightweight access points.

Note When NCS polls, some data may change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.The following information is available:

- General
  - Rogue MAC Address—Media Access Control address of the adhoc rogue.
  - Vendor—Adhoc rogue vendor name or Unknown.
  - On Network—Indicates how the rogue detection occurred.

    Controller—The controller detected the rogue (Yes or No).

    Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
  - Owner—Indicates the owner or left blank.
  - Acknowledged—Indicates whether or not the alarm is acknowledged by the user.

You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in NCS and you can search for all Acknowledged alarms using the alarm search functionality. See "Acknowledging Alarms" for more information.

- State—Indicates the state of the alarm. Possible states for adhoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
- SSID—Service Set Identifier being broadcast by the adhoc rogue radio. (Blank if SSID is not broadcast.)
- Channel Number—Indicates the channel of the adhoc rogue.
- Containment Level—Indicates the containment level of the adhoc rogue or Unassigned.
- Radio Type—Lists all radio types applicable to this adhoc rogue.
- Strongest AP RSSI—Indicates the strongest received signal strength indicator for this NCS (including all detecting access points for all controllers and across all detection times).
- No. of Rogue Clients—Indicates the number of rogue clients associated to this adhoc.

Note This number comes from the NCS database It is updated every two hours. From the **Monitor** > **Alarms** > **Alarm Details** page, this number is a real-time number. It is updated each time you open the Alarm Details page for this rogue access point.

- Created—Indicates when the alarm event was created.
- Modified—Indicates when the alarm event was modified.
- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).

  NMS (Network Management System - NCS)—Generated through polling. NCS periodically polls the controllers and generates events. NCS generates events when the traps are disabled or when the traps are lost for those events. In this case "Generated by" will be NMS

  Trap—Generated by the controller. NCS process these traps and raises corresponding events for them. In this case "Generated by" will be Controller.
- Severity—Indicates the severity of the alarm including:

Icon	Meaning
⊗	Critical
▽	Major
⚠	Minor
◆	Warning

Icon	Meaning
ⓘ	Info
☑	Clear—Displays if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from NCS after 30 days.

  - Previous Severity—The previous severity of the alarm: Critical, Major, Minor, Clear. Color coded.

- Annotations—Enter any new notes in this box and click **Add** to update the alarm.
- Message—Displays descriptive information about the alarm.
- Help—Displays the latest information about the alarm.
- Event History—Click to access the **Monitor** > **Events** page. See "Monitoring Events" for more information.
- Annotations—Lists existing notes for this alarm.

Searching Rogue Clients Using Advanced Search

When the access points on your wireless LAN are powered up and associated with controllers, NCS immediately starts listening for rogue access points. When a controller detects a rogue access point, it immediately notifies NCS, which creates a rogue access point alarm.

Follow these steps to find rogue access point alarms using Advanced Search.

Step 1 Click **Advanced Search** in the top right-hand corner of the NCS main page.

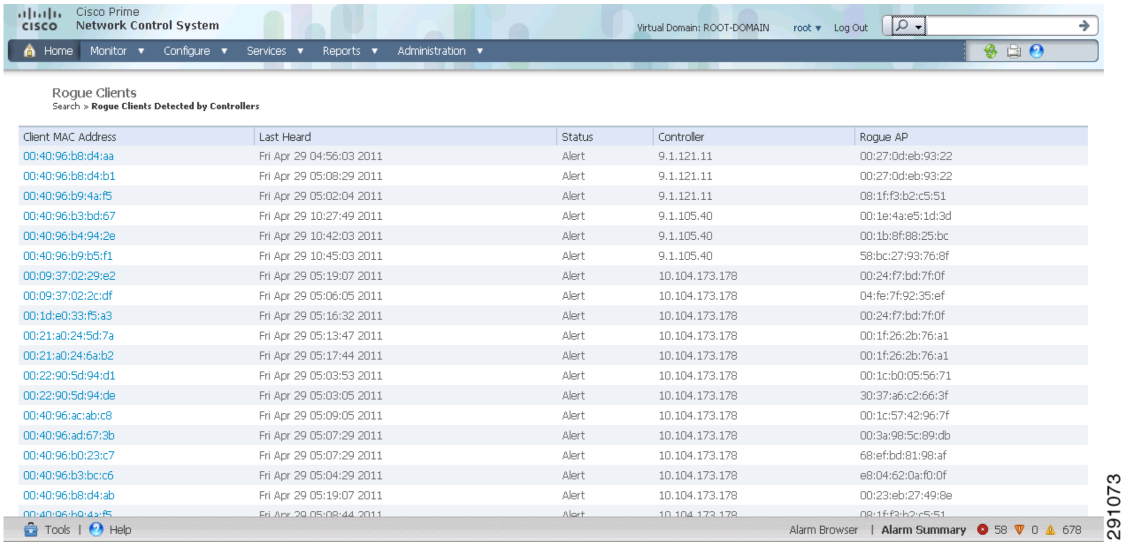
Step 2 Choose **Rogue Client** from the Search Category drop-down list.

Step 3 (optional) You can filter the search even further with the other search criteria if desired.

Step 4 Click **Search**.

Step 5 The list of rogue clients appears (see Figure 5-3).

Figure 5-3 Rogue Clients Page

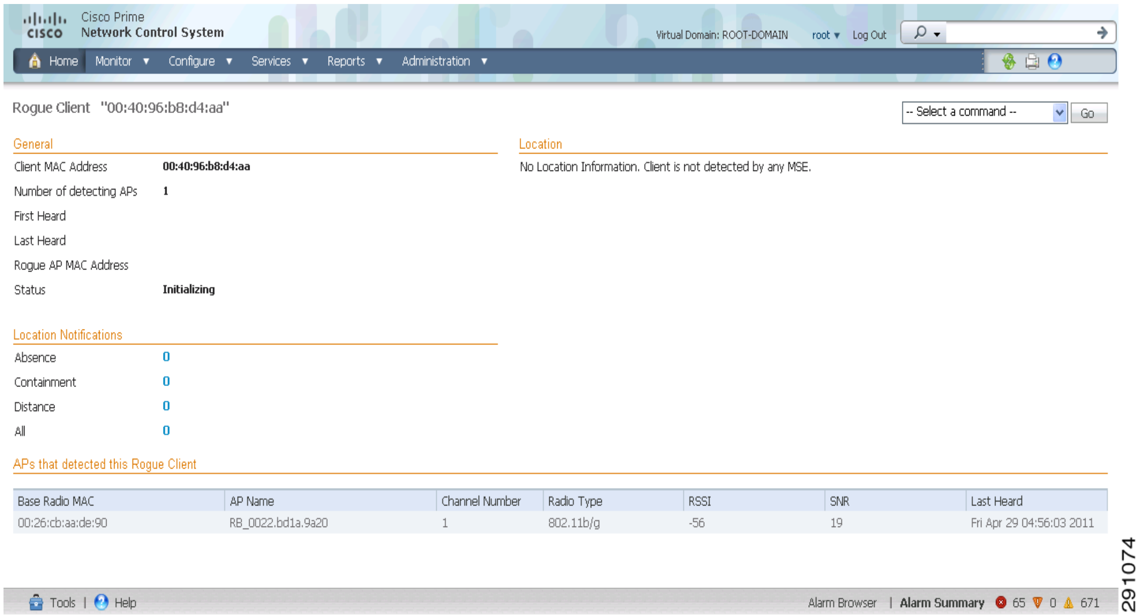


Rogue Clients
Search > **Rogue Clients Detected by Controllers**

Client MAC Address	Last Heard	Status	Controller	Rogue AP
00:40:96:b8:d4:aa	Fri Apr 29 04:56:03 2011	Alert	9.1.121.11	00:27:0d:eb:93:22
00:40:96:b8:d4:b1	Fri Apr 29 05:08:29 2011	Alert	9.1.121.11	00:27:0d:eb:93:22
00:40:96:b9:4a:f5	Fri Apr 29 05:02:04 2011	Alert	9.1.121.11	08:1f:f3:b2:c5:51
00:40:96:b3:bd:67	Fri Apr 29 10:27:49 2011	Alert	9.1.105.40	00:1e:4a:e5:1d:3d
00:40:96:b4:94:2e	Fri Apr 29 10:42:03 2011	Alert	9.1.105.40	00:1b:8f:88:25:bc
00:40:96:b9:b5:f1	Fri Apr 29 10:45:03 2011	Alert	9.1.105.40	58:bc:27:93:76:8f
00:09:37:02:29:e2	Fri Apr 29 05:19:07 2011	Alert	10.104.173.178	00:24:f7:bd:7f:0f
00:09:37:02:2c:df	Fri Apr 29 05:06:05 2011	Alert	10.104.173.178	04:fe:7f:92:35:ef
00:1d:e0:33:f5:a3	Fri Apr 29 05:16:32 2011	Alert	10.104.173.178	00:24:f7:bd:7f:0f
00:21:a0:24:5d:7a	Fri Apr 29 05:13:47 2011	Alert	10.104.173.178	00:1f:26:2b:76:a1
00:21:a0:24:6a:b2	Fri Apr 29 05:17:44 2011	Alert	10.104.173.178	00:1f:26:2b:76:a1
00:22:90:5d:94:d1	Fri Apr 29 05:03:53 2011	Alert	10.104.173.178	00:1c:b0:05:56:71
00:22:90:5d:94:de	Fri Apr 29 05:03:05 2011	Alert	10.104.173.178	30:37:a6:c2:66:3f
00:40:96:ac:ab:c8	Fri Apr 29 05:09:05 2011	Alert	10.104.173.178	00:1c:57:42:96:7f
00:40:96:ad:67:3b	Fri Apr 29 05:07:29 2011	Alert	10.104.173.178	00:3a:98:5c:89:db
00:40:96:b0:23:c7	Fri Apr 29 05:07:29 2011	Alert	10.104.173.178	68:ef:bd:81:98:af
00:40:96:b3:bc:c6	Fri Apr 29 05:04:29 2011	Alert	10.104.173.178	e8:04:62:0a:f0:0f
00:40:96:b8:d4:ab	Fri Apr 29 05:19:07 2011	Alert	10.104.173.178	00:23:eb:27:49:8e
00:40:96:b9:4a:f5	Fri Apr 29 05:08:44 2011	Alert	10.104.173.178	08:1f:f3:b2:c5:51

Step 6 Choose a rogue client by clicking a client MAC address. The Rogue Client detail page appears (see Figure 5-4).

Figure 5-4 Rogue Client Detail Page



Rogue Client "00:40:96:b8:d4:aa"

-- Select a command -- Go

General

Client MAC Address	**00:40:96:b8:d4:aa**
Number of detecting APs	**1**
First Heard	
Last Heard	
Rogue AP MAC Address	
Status	**Initializing**

Location

No Location Information. Client is not detected by any MSE.

Location Notifications

Absence	0
Containment	0
Distance	0
All	0

APs that detected this Rogue Client

Base Radio MAC	AP Name	Channel Number	Radio Type	RSSI	SNR	Last Heard
00:26:cb:aa:de:90	RB_0022.bd1a.9a20	1	802.11b/g	-56	19	Fri Apr 29 04:56:03 2011

Step 7 To modify the alarm, choose one of these commands from the Select a command drop-down list, and click **Go**.

- Set State to 'Unknown-Alert'—Tags the ad hoc rogue as the lowest threat, continues to monitor the ad hoc rogue, and turns off containment.
- 1 AP Containment through 4 AP Containment—Indicates the number of access points (1-4) in the vicinity of the rogue unit that send dauthenticate and disassociate messages to the client devices that are associated to the rogue unit.

- Map (High Resolution)—Displays the current calculated rogue location on the Maps > Building Name > Floor Name page.
- Location History—Displays the history of the rogue client location based on RF fingerprinting.

Note The client must be detected by an MSE for the location history to appear.

Monitoring Rogue Access Point Location, Tagging, and Containment

When the Cisco Unified Network Solution is monitored using NCS, NCS generates the flags as rogue access point traps and displays the known rogue access points by MAC address. The operator can then display a map showing the location of the access points closest to each rogue access point. The next step is to mark them as Known or Acknowledged rogue access points (no further action), Alert rogue access points (watch for and notify when active), or Contained rogue access points (have between one and four access points discourage rogue access point clients by sending the clients deauthenticate and disassociate messages whenever they associate with the rogue access point).

This built-in detection, tagging, monitoring, and containment capability enables system administrators to take appropriate action:

- Locate rogue access points
- Receive new rogue access point notifications, eliminating hallway scans
- Monitor unknown rogue access points until they are eliminated or acknowledged
- Determine the closest authorized access point, making directed scans faster and more effective
- Contain rogue access points by sending their clients deauthenticate and disassociate messages from one to four access points. This containment can be done for individual rogue access points by MAC address or can be mandated for all rogue access points connected to the enterprise subnet.
- Tag rogue access points:
  - Acknowledge rogue access points when they are outside of the LAN and do not compromise the LAN or wireless LAN security
  - Accept rogue access points when they do not compromise the LAN or wireless LAN security
  - Tag rogue access points as unknown until they are eliminated or acknowledged
- Tag rogue access points as contained and discourage clients from associating with the rogue access points by having between one and four access points transmit deauthenticate and disassociate messages to all rogue access point clients. This function applies to all active channels on the same rogue access point.

Detecting Access Points

Use the Detecting Access Points feature to view information about the Cisco lightweight access points that are detecting a rogue access point.

To access the Rogue AP Alarms details page, follow these steps:

Step 1 To display the Rogue AP Alarms page, do one of the following:

- Perform a search for rogue APs. See "Using the Search Feature" for more information about the search feature.
- From the NCS home page, click the Security dashboard. This dashboard displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
- Click the **Malicious AP** number link in the Alarm Summary box.

Step 2 From the Rogue AP Alarms page, click the Rogue MAC Address for the applicable rogue access point. The Rogue AP Alarms details page appears.

Step 3 From the Select a command drop-down list, choose **Detecting APs**.

Step 4 Click **Go**.

Click a list item to display data about that item:

- AP Name
- Radio
- Map Location
- SSID—Service Set Identifier being broadcast by the rogue access point radio.
- Channel Number—Which channel the rogue access point is broadcasting on.
- WEP—Enabled or disabled.
- WPA—Enabled or disabled.
- Pre-Amble—Long or short.
- RSSI—Received signal strength indicator in dBm.
- SNR—Signal-to-noise ratio.
- Containment Type—Type of containment applied from this access point.
- Containment Channels—Channels that this access point is currently containing.

Monitoring Rogue Alarm Events

The Events page enables you to review information about rogue alarm events. NCS generates an event when a rogue access point is detected or if you make manual changes to a rogue access point (such as changing its state). The Rogue AP Events list page displays all rogue access point events.

To access the Rogue AP Events list page, follow these steps:

Step 1 Do one of the following:

- Perform a search for rogue access point events using the Advanced Search feature of NCS. See "Advanced Search" for more information.
- From the Rogue AP Alarms details page, click **Event History** from the Select a command drop-down list. See "Viewing Rogue AP Alarm Details" for more information.

Step 2 The Rogue AP Events list page displays the following event information.

- Severity—Indicates the severity of the alarm including:

Icon	Meaning
⊗	Critical
▽	Major
⚠	Minor
◆	Warning
ℹ	Info

- Rogue MAC Address—Click the rogue MAC address to view the Rogue AP Event Details page. See "Viewing Rogue AP Event Details" for more information.
- Vendor—Rogue access point vendor name or Unknown.
- Classification Type—Malicious, Friendly, or Unclassified.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Date/Time—The date and time that the event was generated.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

Viewing Rogue AP Event Details

To view rogue access point event details, follow these steps:

Step 1 From the Rogue AP Events list page, click the Rogue MAC Address link.

Step 2 The Rogue AP Events Details page displays the following information:

- Rogue MAC Address
- Vendor—Rogue access point vendor name or Unknown.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Classification Type—Malicious, Friendly, or Unclassified.

- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Channel Number—The channel on which the rogue access point is broadcasting.
- Containment Level—Indicates the containment level of the rogue access point or Unassigned.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Created—The date and time that the event was generated.
- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
  - NMS (Network Management System - NCS)—Generated through polling. NCS periodically polls the controllers and generates events. NCS generates events when the traps are disabled or when the traps are lost for those events. In this case "Generated by" will be NMS.
  - Trap—Generated by the controller. NCS process these traps and raises corresponding events for them. In this case "Generated by" will be Controller.
- Device IP Address
- Severity—Indicates the severity of the alarm including:

Icon	Meaning
⊗	Critical
▼	Major
⚠	Minor
◆	Warning
ℹ	Info
☑	Clear—Displays if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from NCS after 30 days.

- Message—Provides details of the current event.

Monitoring Adhoc Rogue Events

The Events page enables you to review information about adhoc rogue events. NCS generates an event when an adhoc rogue is detected or if you make manual changes to an adhoc rogue (such as changing its state). The Adhoc Rogue Events list page displays all adhoc rogue events.

To access the Rogue AP Events list page, follow these steps:

Step 1 Do one of the following:

- Perform a search for adhoc rogues events using the Advanced Search feature of NCS. See "Advanced Search" for more information.
- From the Adhoc Rogue Alarms details page, click **Event History** from the Select a command drop-down list. See "Viewing Adhoc Rogue Alarm Details" for more information.

Step 2 The Rogue AP Events list page displays the following event information.

- Severity—Indicates the severity of the alarm including:

Icon	Meaning
⊗	Critical
▼	Major
⚠	Minor
◆	Warning
ⓘ	Info

- Rogue MAC Address—Click the rogue MAC address to view the Rogue AP Event Details page. See "Viewing Adhoc Rogue Event Details" for more information.
- Vendor—Rogue access point vendor name or Unknown.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Date/Time—The date and time that the event was generated.
- State—Indicates the state of the alarm. Possible states for adhoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

Viewing Adhoc Rogue Event Details

To view rogue access point event details, follow these steps:

Step 1 From the Rogue AP Events list page, click the Rogue MAC Address link.

Step 2 The Rogue AP Events Details page displays the following information:

- Rogue MAC Address
- Vendor—Rogue access point vendor name or Unknown.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- State—Indicates the state of the alarm. Possible states for adhoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Channel Number—The channel on which the rogue access point is broadcasting.
- Containment Level—Indicates the containment level of the rogue access point or Unassigned.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Created—The date and time that the event was generated.
- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
  - NMS (Network Management System - NCS)—Generated through polling. NCS periodically polls the controllers and generates events. NCS generates events when the traps are disabled or when the traps are lost for those events. In this case “Generated by” will be NMS
  - Trap—Generated by the controller. NCS process these traps and raises corresponding events for them. In this case “Generated by” will be Controller.
- Device IP Address
- Severity—Indicates the severity of the alarm including:

Icon	Meaning
⊗	Critical
▽	Major
⚠	Minor
◈	Warning
ℹ	Info
☑	Clear—Displays if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from NCS after 30 days.

- Message—Provides details of the current event.

Monitoring RFID Tags

The **Monitor** > RFID **Tags** page allows you to monitor tag status and location on NCS maps as well as review tag details.

Note This page is only available in the Location version of NCS.

This section provides information on the tags detected by the location appliance.

Choose **Monitor > RFID Tags** to access this section. By default, Tag Summary page is displayed.

- Tag Summary
- Searching Tags
- Viewing RFID Tag Search Results
- Viewing Tag List

Tag Summary

Choose **Monitor > RFID Tags** to access this page.

This page provides information on the number of tags that are detected by MSE. The following parameters are displayed on the main data area:

- MSE Name—Name of the MSE device.
- Total Tags—Click the number to view tag details. Clicking on the number gives the list of tags located by the MSE. Click on a mac address gives the tag details pertaining to that mac address.

Searching Tags

Use the NCS Advanced Search feature to find specific or all tags.

To search for tags in NCS, follow these steps:

Step 1 Click **Advanced Search**.

Step 2 Select **Tags** from the Search Category drop-down list.

Step 3 Identify the applicable tag search parameters including:

- Search By—Choose All Tags, Asset Name, Asset Category, Asset Group, MAC Address, Controller, MSE, Floor Area, or Outdoor Area.

  Note Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.

- Search In—Choose MSEs or NCS Controllers.
- Last detected within—Choose a time increment from 5 minutes to 24 hours. The default is 15 minutes.
- Tag Vendor—Select the check box and choose Aeroscout, G2, PanGo, or WhereNet.
- Telemetry Tags only—Check the Telemetry Tags only to search tags accordingly.

Step 4 Click **Go**.

Viewing RFID Tag Search Results

Use the NCS Advanced Search feature located at the top right of the NCS window to search for tags by asset type (name, category and group), by MAC address, by system (controller or location appliance), and by area (floor area and outdoor area).

Note Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.

You can further refine your search using the Advanced search parameters and save the search criteria for future use. Saved search criteria can be retrieved from the Saved Searches located in the navigation bar.

See "Advanced Search" or "Saved Searches" for additional information.

When you click the MAC address of a tag location in a search results page, the following details display for the tag:

- Tag vendor

  Note Option does not display when Asset Name, Asset Category, Asset Group or MAC Address are the search criteria for tags.

- Controller to which tag is associated
- Telemetry data (CCX v1 compliant tags only)
  - Telemetry data displayed is vendor-specific; however, some commonly reported details are GPS location, battery extended information, pressure, temperature, humidity, motion, status, and emergency code.

    Note The Telemetry data option only appears when MSE (select for location servers), Floor Area, or Outdoor Area are selected as the Search for tags by option.

    Note Only those vendor tags that support telemetry appear.

- Asset Information (Name, Category, Group)
- Statistics (bytes and packets received)
- Location (Floor, Last Located, MSE, map)

- Location Notification (Absence, Containment, Distance, All)

Note Telemetry data displayed is vendor-specific; however, some commonly reported details are GPS location, battery extended information, pressure, temperature, humidity, motion, status, and emergency code.

- Emergency Data (CCX v1 compliant tags only)

Viewing Tag List

Click the Total Tags number link to view the Tags List for the applicable device name. The Tag List contains the following information:

- MAC Address
- Asset Name
- Asset Group
- Asset Category
- Vendor Name
- Mobility Services Engine
- Controller
- Battery Status
- Map Location

Monitoring Chokepoints

Chokepoints are installed and configured as recommended by the Chokepoint vendor. After the chokepoint installation is complete and operational, the chokepoint can be added to NCS and placed on Floor Maps. They are pushed to the Location Server during synchronization.

Choose **Monitor > Chokepoints** to access this section. A page appears displaying a list of found chokepoints. Clicking a the link under Map Location for a particular chokepoint displays a map that shows the location of the chokepoint.

The following parameters are displayed:

- MAC Address—The MAC address of the chokepoint.
- Chokepoint Name—The user-defined name of the chokepoint.
- Entry/Exit Chokepoint—Indicates whether or not the chokepoint is an entry/exit chokepoint.
- Range—The range of the chokepoint in feet.
- Static IP—The static IP address of the chokepoint.
- Map Location—A link to a map showing the location of the chokepoint.

Performing a Chokepoint Search

An advanced search allows you to search for chokepoints.

To perform an advanced search for a chokepoint in NCS, follow these steps:

Step 1 Click **Advanced Search** located in the top right corner of NCS.

Step 2 From the New Search page, select **Chokepoint** from the Search Category drop-down list.

Step 3 Select the method by which you want to search (by MAC address or chokepoint name) from the Search for Chokepoint by drop-down list.

Step 4 Enter the MAC address or chokepoint name, depending on the search method selected.

Step 5 Click **Search**.

Monitoring Interferers

The **Monitor** > **Interferer** page allows you to monitor interference devices detected by the CleanAir enabled access points.

This section provides information on the interferers detected by the CleanAir enabled access points. By default, the Monitoring AP Detected Interferers page is displayed.

- Monitoring AP Detected Interferers, page 5-116
- Monitoring AP Detected Interferer Details, page 5-117
- Monitoring AP Detected Interferer Details Location History, page 5-118
- Configuring the Search Results Display, page 5-119

Monitoring AP Detected Interferers

Choose **Monitor** > **Interferers** to view all the interfering devices detected by the CleanAir enabled access points on your wireless network. This page enables you to view a summary of the interfering devices including the following default information:

- Interferer ID—A unique identifier for the interferer. This is a pseudo-randomly generated ID. Though it is similar to a MAC address, it is not a real address, which you can use to find the interfering device. Click this link to know more about the interferer.
- Type—Indicates the category of the interferer. Click to read more about the type of device. A pop-up page appears displaying more details. The categories include:
  - Bluetooth link—A Bluetooth link (802.11b/g/n only)
  - Microwave Owen—A microwave oven (802.11b/g/n only)
  - 802.11 FH—An 802.11 frequency-hopping device (802.11b/g/n only)
  - Bluetooth Discovery—A Bluetooth discovery (802.11b/g/n only)
  - TDD Transmitter—A time division duplex (TDD) transmitter
  - Jammer—A jamming device
  - Continuous Transmitter—A continuous transmitter
  - DECT-like Phone—A digital enhanced cordless communication (DECT)-compatible phone
  - Video Camera—A video camera

  - 802.15.4—An 802.15.4 device (802.11b/g/n only)
  - WiFi Standard—A device using standard Wi-Fi channels
  - WiFi Inverted—A device using spectrally inverted Wi-Fi signals
  - WiFi Invalid Channel—A device using non-standard Wi-Fi channels
  - SuperAG—An 802.11 SuperAG device
  - Canopy—A Motorola Canopy device
  - Radar—A radar device (802.11a/n only)
  - XBox—A Microsoft Xbox (802.11b/g/n only)
  - WiMAX Mobile—A WiMAX mobile device (802.11a/n only)
  - WiMAX Fixed—A WiMAX fixed device (802.11a/n only)
  - WiFi AOCI—A WiFi device with AOCI
  - Unclassified
- Status—Indicates the status of the interfering device.
  - Active—Indicates that the interferer is currently being detected by the CleanAir capable access point.
  - Inactive—Indicates that the interferer is no longer being detected by the CleanAir capable access point or no longer reacheable by NCS.
- Severity—Displays the severity ranking of the interfering device.
- Affected Band—Displays the band in which this device is interfering.
- Affected Channels—Displays the affected channels.
- Duty Cycle (%)—The duty cycle of interfering device in percentage.
- Discovered—Displays the time at which it was discovered.
- Last Updated—The last time the interference was detected.
- Floor—The location where the interfering device is present.

Monitoring AP Detected Interferer Details

Choose **Monitor** > **Interferers** > <Interferer ID> to view this page. This page enables you to view the details of the interfering devices detected by the access points. This page provides the following details about the interfering device.

- Interferer Properties
  - Type—Displays the type of the interfering device detected by the AP.
- Status—The status of the interfering device. Indicates the status of the interfering device.
  - Active—Indicates that the interferer is currently being detected by the CleanAir capable access point.
  - Inactive—Indicates that the interferer is no longer being detected by the CleanAir capable access point or no longer reachable by NCS.
  - Severity—Displays the severity ranking of the interfering device.
  - Duty Cycle (%)—The duty cycle of interfering device in percentage.
  - Affected Band—Displays the band in which this device is interfering.

  - Affected Channels—Displays the affected channels.
  - Discovered—Displays the time at which it was discovered.
  - Last Updated—The last time the interference was detected.
- Location
  - Floor—The location where this interfering device was detected.
  - Last Located At—The last time where the interfering device was located.
  - On MSE—The Mobility Server Engine on which this interference device was located.
- Clustering Information
  - Clustered By—Displays the IP address of the controller or the MSE that clustered the interferer information from the access point.
  - Detecting APs—Displays the details of the access point that has detected the interfering device. The details include: Access Point Name (Mac), Severity, and Duty Cycle(%).
- Details—Displays a short description about the interfering type.

Select a command

The Select a command drop-down list provides access to the location history of the interfering device detected by the access point. See Monitoring AP Detected Interferer Details Location History.

Monitoring AP Detected Interferer Details Location History

Choose **Monitor > Interferers > <Interference Device ID**, select **Location History** from the Select a command drop-down list, and click **Go** to view this page.

- Interferer Information—Displays the basic information about the interfering device.
  - Data Collected At—The time stamp at which the data was collected.
  - Type—The type of the interfering device.
  - Severity—The severity index of the interfering device.
  - Duty Cycle—The duty cycle (in percentage) of the interfering device.
  - Affected Channels—A comma separated list of the channels affected.
- Interferer Location History—Displays the location history of the interfering devices.
  - Time Stamp
  - Floor
- Clustering Information
  - Clustered By
- Detecting APs
  - AP Name—The access point that detected the interfering device.
  - Severity—The severity index of the interfering device.
  - Duty Cycle(%)—The duty cycle (in percentage) of the interfering device.
- Location
  - Location Calculated At—Displays the time stamp at which this information was generated.

- Floor—Displays location information of the interfering device.
- A graphical view of the location of the interfering device is displayed in a map. Click the Enlarge link to view an enlarged image.

Configuring the Search Results Display

The Edit View page allows you to add, remove, or reorder columns in the AP Detected Interferers Summary page.

To edit the columns in the AP Detected Interferers page, follow these steps:

Step 1 Choose **Monitor > Interferers**. The AP Detected Interferers page appears showing details of the interferers detected by the CleanAir enabled access points.

Step 2 Click the **Edit View** link.

Step 3 To add an additional column to the access points table, click to highlight the column heading in the left column. Click **Show** to move the heading to the right column. All items in the right column are displayed in the table.

Step 4 To remove a column from the access points table, click to highlight the column heading in the right column. Click **Hide** to move the heading to the left column. All items in the left column are not displayed in the table.

Step 5 Use the **Up/Down** buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click **Up** or **Down** to move it higher or lower in the current list.

Step 6 Click **Reset** to restore the default view.

Step 7 Click **Submit** to confirm the changes.

Monitoring Spectrum Experts

A Spectrum Expert client acts as a remote interference sensor and sends dynamic interference data to NCS. This feature allows the NCS to collect and archive and monitor detailed interferer and air quality data from Spectrum Experts in the network.

To access the Monitor Spectrum Experts page, follow these steps:

Step 1 Choose **Monitor > Spectrum Experts**.

Step 2 From the left sidebar menu, you can access the Spectrum Experts Summary page and the Interferers Summary page.

Spectrum Experts Summary

The **Spectrum Experts** > **Summary** page is the default page and provides a table of the Spectrum Experts added to the system. The table provides the following Spectrum Expert information:

- Hostname—Displays the hostname or IP Address depending on how it was added. Click the hostname to access the Spectrum Experts Details page.

- Active Interferers—Indicates the current number of interferes being detected by the Spectrum Experts.
- Affected APs—The number of access points seen by the Spectrum Expert that are potentially affected by detected interferers.
- Alarms—The number of active interference traps sent by the Spectrum Expert. Click to access the Alarm page that is filtered to the active alarms for this Spectrum Expert.
- Reachability Status—Indicates “Reachable” in green if the Spectrum Expert is running and sending data to NCS; otherwise indicates “Unreachable” in red.
- Location—When the Spectrum is a wireless client, a link is available that displays the location of the Spectrum Expert. A red box around the Spectrum Expert indicates the effective range. Click to access the nearest mapped access point.

Interferers Summary

The **Interferers** > **Summary** page displays a list of all the Interferers detected over a 30 day interval. The table provides the following Interferers information:

- Interferer ID—An identifier that is unique across different spectrum experts. This is a pseudo-randomly generated ID. Though it is similar to a MAC address, it is not a real address, which you can use to find the interfering device.
- Category—Indicates the category of the interferer. Categories include: Bluetooth, Cordless Phones, Microwave Ovens, 802.11 FH, Generic - Fixed-Frequency, Jammers, Generic - Frequency-Hopped, Generic - Continuous.
- Type—Indicates the type of Interferer. Click to access a pop-up description of the type.
- Status—Indicates Active or Inactive.
  - Active—Indicates that the interferer is currently being detected by a spectrum expert.
  - Inactive—Indicates that the interferer is no longer detected by a spectrum expert or the spectrum expert that saw the interferer is no longer reachable by NCS.
- Discover Time—Indicates the time of discovery.
- Affected Channels—Identifies affected channels.
- Number of APs Affected—An access point is listed as Affected if the following conditions are met:
  - The access point is managed by NCS.
  - The spectrum expert detects the access point.
  - The spectrum expert detects an interferer on the serving channel of the access point.
- Power—Indicated in dBm.
- Duty Cycle—Indicated in percentage.

  Note 100% indicates the worst value.

- Severity—Indicates the severity ranking of the Interferer.

  Note 100% indicates the worst value where 0 indicates no interference.

Interferers Search

Use the NCS Search feature to find specific Interferers or to create and save custom searches. See one of the following topics for additional information:

- Using the Search Feature
- Quick Search
- Advanced Search
- Saved Searches

Spectrum Experts Details

The Spectrum Expert Details page provides all interference details from a single Spectrum Expert. This page updates every 20 seconds providing a real-time look at what is happening on the remote Spectrum Expert and includes the following items:

- Total Interferer Count—As seen by the specific Spectrum Expert.
- Active Interferers Count Chart—Displays a pie chart that groups interferes by category.
- Active Interferer Count Per Channel—Displays the number of interferes grouped by category on different channels.
- AP List—Provides a list of access points detected by the Spectrum Expert that are on channels that have active interferers detected by the Spectrum Expert on those channels.
- Affected Clients List—Provides a list of clients that are currently authenticated/associated to the radio of one of the access points listed in the access point list.

Monitoring WiFi TDOA Receivers

To monitor Wi-Fi TDOA receivers, follow these steps:

Step 1 Choose **Monitor > WiFi TDOA Receivers**. The WiFi TDOA Receiver summary page appears showing all mapped WiFI TDOA receivers.

Step 2 To refine the search criteria when an extensive lists appears, you can search by MAC address or location sensor name.

a. To initiate a search for a TDOA receiver by its MAC address, click the **Advanced Search** link in the NCS window. Select **WiFi TDOA Receiver** from the Search Category drop-down list and **MAC Address** from the Search by drop-down list. Enter the MAC address of the TDOA receiver in the available text box and click **Search**.

b. To initiate a search for a TDOA receiver by its name, select **Advanced Search** link in the NCS window. Select **WiFi TDOA Receiver** from the Search Category drop-down list and **WiFi TDOA Receivers** from the Search by drop-down list. Enter the name of the TDOA receiver in the available text box and click **Search**.

If no match exists, then a message indicating that appears in the page. Otherwise the search result displays.

Note See "Using the Search Feature" or "Advanced Search" for more information on the NCS Search feature.

The WiFi TDOA Receivers page displays the following information:

- MAC Address
- WiFi TDOA Receiver Name
- Static IP—Static IP address of the WiFi TDOA receiver.
- Oper Status—Up or down.
- Map Location—Click the Map Location link to view the floor map for this WiFi TDOA receiver. See "Floor Area" for more information on NCS floor maps.

Note See "Configuring WiFi TDOA Receivers" for more information on adding, configuring, and editing WiFi TDOA receivers.

Monitoring Radio Resource Management (RRM)

The operating system security solution uses the radio resource management (RRM) function to continuously monitor all nearby access points, automatically discover rogue access points, and locate them as described in the "" section.

Radio Resource Management (RRM) built into the Cisco Unified Wireless Network monitors and dynamically corrects performance issues found in the RF environment.

NCS would receive traps whenever a change in the transmit power of the access point or channel occurred. These trap events or similar events such as RF regrouping were logged into NCS events as informational and were maintained by the event dispatcher. The reason behind the transmit power or channel changes (such as signals from neighboring access points, interference, noise, load, and the like) were not evident. You could not view these events and statistics to then perform troubleshooting practices.

Radio Resource Management (RRM) statistics helps to identify trouble spots and provides possible reasons for channel or power level changes. The dashboard provides network-wide RRM performance statistics and predicts reasons for channel changes based on grouping the events together (worst performing access points, configuration mismatch between controllers in the same RF group, coverage holes that were detected by access points based on threshold, pre-coverage holes that were detected by controllers, ratios of access points operating at maximum power, and so on).

Note The RRM dashboard information is only available for lightweight access points.

- Channel Change Notifications
- Transmission Power Change Notifications
- RF Grouping Notifications
- Viewing the RRM Dashboard

Channel Change Notifications

Notifications are sent to the NCS RRM dashboard when a channel change occurs. Channel changes depend on the dynamic channel assignment (DCA) configuration where the mode can be set to auto or on demand. When the mode is *auto*, channel assignment is periodically updated for all lightweight access points which permit this operation. When the mode is set to *on demand*, channel assignments are updated based upon request. If the DCA is static, no dynamic channel assignments occur, and values are set to their global default.

When a channel change trap is received and a channel change had occurred earlier, the event is marked as Channel Revised; otherwise, the event is marked as Channel Changed. Each event for channel change can be caused by multiple reasons. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur. For example, suppose a channel change is caused by signal, interference, or noise. When the reason code is received in the notification, the reason code is refactored across the reasons. If three reasons caused the event to occur, the reason code is refactored to 1/3 or 0.33 per reason. If ten channel change events are received with the same reason code, all of the three reasons are equally factored to determine the cause of the channel change.

Transmission Power Change Notifications

Notifications are sent to the NCS RRM dashboard when transmission power changes occur. Each event for transmit power changes is caused by multiple reasons. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur.

RF Grouping Notifications

When RRM is run on the controller, dynamic grouping is done, and a new group leader is chosen. Dynamic grouping has three modes: Automatic, Off and Leader. When the grouping is Off, no dynamic grouping occurs, and each switch optimizes only its own lightweight access point parameters. When the grouping is Automatic, switches form groups and elect leaders to perform better dynamic parameter optimization. With grouping automatic, configured intervals (in seconds) represent the period with which the grouping algorithm is run. (Grouping algorithms also run when the group contents change and automatic grouping is enabled.)

Viewing the RRM Dashboard

The RRM dashboard is accessed by choosing **Monitor > RRM**.

The dashboard is made up of the following parts:

- The RRM RF Group Summary shows the number of different RF groups.

  Note To get the latest number of RF Groups, you have to run the configuration sync background task.

- The RRM Statistics portion shows network-wide statistics
- The Channel Change Reason portion shows why channels changed for all 802.11a/b/g/n radios.
  - Signal—The channel changed because it improved the channel quality for some other neighbor radio(s). Improving the channel quality for some other neighbor radio(s) improved the channel plan of the system as evaluated by the algorithm.
  - Wifi Interference

- Load
- Radar
- Noise
- Persistent Non-Wifi Interference
- Major Air Quality Event
- Other

- The Channel Change shows all events complete with causes and reasons.
- The Configuration Mismatch portion shows comparisons between leaders and members.
- The Coverage Hole portion rates how severe the coverage holes are and gives their location.
- The Percent Time at Maximum Power shows what percent of time the access points were at maximum power and gives the location of those access points.

The following statistics are displayed:

- Total Channel Changes—The sum total of channel changes across 802.11a/b/g/n radios, irrespective of whether the channel was updated or revised. The count is split over a 24-hour and 7-day period. If you click the percentages link or the link under the 24-hour column, a page with details for that access point only appears.
- Total Configuration Mismatches—The total number of configuration mismatches detected over a 24-hour period.
- Total Coverage Hole Events—The total number of coverage hole events over a 24-hour and 7-day period.
- Number of RF Groups—The total number of RF groups (derived from all the controllers which are currently managed by NCS).
- Configuration Mismatch—The configuration mismatch over a 24-hour period by RF group with details on the group leader.
- APs at MAX Power—The percentage of access points with 802.11a/n radios as a total percentage across all access points which are at maximum power. The maximum power levels are preset and are derived with reference to the preset value.

Note Maximum power is shown in three areas of the RRM dashboard. This maximum power portion shows the current value and is poll driven.

- Channel Change Causes—A graphical bar chart for 802.11a/n radios. The chart is factored based on the reason for channel change. The chart is divided into two parts, each depicting the percentage of weighted reasons causing the event to occur over a 24-hour and 7-day period. Each event for channel change can be caused by multiple reasons, and the weight is equally divided across these reasons. The net reason code is factored and equated to one irrespective of the number of reasons for the event to occur.
- Channel Change - APs with channel changes—Each event for channel change includes the MAC address of the lightweight access point. For each reason code, you are given the most channel changes that occurred for the 802.11a/n access point based on the weighted reason for channel events. This count is split over a 24-hour and 7-day period.
- Coverage Hole - APs reporting coverage holes—The top five access points filtered by IF Type 11 a/n which triggered a coverage hole event (threshold based) are displayed.

- Aggregated Percent Max Power APs—A graphical progressive chart of the total percentage of 802.11a/n lightweight access points which are operating at maximum power to accommodate coverage holes events. The count is split over a 24-hour and 7-day period.

Note This maximum power portion shows the values from the last 24 hours and is poll driven. This occurs every 15 minutes or as configured for radio performance.

- Percent Time at Maximum Power—A list of the top five 802.11a/n lightweight access points which have been operating at maximum power.

Note This maximum power portion shows the value from the last 24 hours and is only event driven.

Monitoring Clients and Users

The Monitor Clients and Users information assists in identifying, diagnosing, and resolving client issues. Using the Monitor Clients and Users feature, you can view a client association history and statistical information. You can also troubleshoot client historical issues. These tools are useful when users complain of network performance as they move throughout a building with their laptop computers. The information may help you assess what areas experience inconsistent coverage and which areas have the potential to drop coverage. See Managing Clients, page 10-1 for more information.

Monitoring Alarms

This section contains the following topics:

- Monitoring Cisco Adaptive wIPS Alarm Details, page 5-140

Alarms and Events Overview

An event is an occurrence or detection of some condition in and around the network. For example, it can be a report about radio interference crossing a threshold, the detection of a new rogue access point, or a controller rebooting.

Events are not generated by a controller for each and every occurrence of a pattern match. Some pattern matches must occur a certain number of times per reporting interval before they are considered a potential attack. The threshold of these pattern matches is set in the signature file. Events can then generate alarms which further can generate e-mail notifications if configured as such.

An alarm is a Cisco NCS response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), the NCS raises an alarm until the resulting condition no longer occurs. For example, an alarm may be raised while a rogue access point is detected, but the alarm terminates after the rogue has not been detected for several hours.

One or more events can result in a single alarm being raised. The mapping of events to alarms is their correlation function. For example, some IDS events are considered to be network wide so all events of that type (regardless of which access point the event is reported from) map to a single alarm. On the other hand, other IDS events are client-specific. For these, all events of that type for a specific client MAC address map to an alarm which is also specific for that client MAC address, regardless of whether multiple access points report the same IDS violation. If the same kind of IDS violation takes place for a different client, then a different alarm is raised.

A NCS administrator currently has no control over which events generate alarms or when they time out. On the controller, individual types of events can be enabled or disabled (such as management, SNMP, trap controls, and so on).

Viewing List of Alarms

Choose **Monitor > Alarms** to access the Alarm Browser page which provides a list of alarms. You can also hover your mouse cursor over **Alarm Browser** in the toolbar at the bottom of the NCS page to view the Alarm Browser page.

The Alarm Browser lists the following information for each alarm:

- Severity—Severity of the alarm which can be:
  - Critical
  - Major
  - Minor
  - Warning
  - Informational
- Status— Status of the alarm.
- Timestamp—Date and time that the alarm occurred.
- Category—Category assigned to the alarm such as rogue AP, controller, switch, and security.
- Condition—Condition that caused the alarm.
- Owner—Name of the person to whom this alarm is assigned, if one was entered.

- Message—Messages about the alarm.
- Failure Source—Indicates the source of the event (including name and/or MAC address).

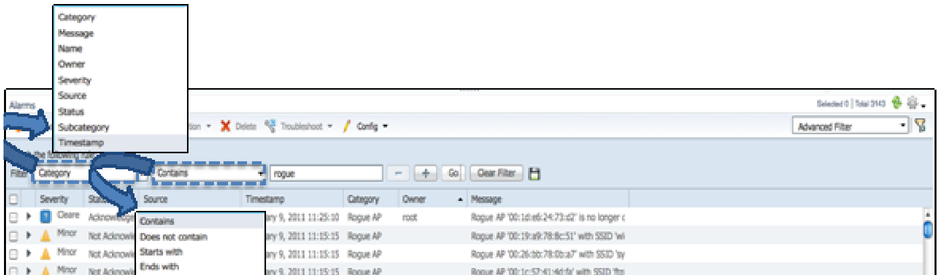
Note By default, acknowledged alarms are not shown in the Alarm Browser page. To change this, select **Administration > Settings > Alarms**, then unselect the Hide Acknowledged Alarms check box. You must unselect the preference of hiding acknowledged alarms if you want acknowledged alarms to show on the NCS Alarm Summary and alarms lists page.

Use the check box to select one or more alarms. To select all alarms displayed in the Alarm Browser, click the topmost box. See Modifying Alarms for more information.

Filtering Alarms

From the **Monitor > Alarms** page, you can filter the alarms that are displayed in the Alarm Browser.

Figure 5-5 Filtering Alarms



Choose **Monitor > Alarms**, then from the Show pulldown menu, select one of the following filters:

- **Quick Filter**—Enter text in any of the boxes to display alarms that contain the text you enter. For example, if you enter **AP** in the Category field, AP and Rogue AP alarms are displayed. It provides an optional filtered view of alarms for wired and wireless alarms.
- **Advance Filter**—This filter provides an advanced alarm search capability. It provides ability to search on specific fields with various conditions like contains, does not contain, starts with, ends with and so on. Additionally advanced filters allows nesting of AND/OR conditions. Select the category and operator, then enter criteria in the text field to compare against, then:
  - Click **+** to add an additional filter or **-** to remove a filter you specified.
  - Click **Go** to apply your filter.
  - Click **Clear Filter** to clear the entries you entered.
  - Click the disc icon to save your filter. Enter a name for the filter you want to save, then click **Save**.

Note When a preset filter is selected and the filter button is clicked, the filter criteria is greyed out. You can only see the filter criteria but will not be able to change it. When '**All**' is selected to view all the entries, clicking on the filter button shows the Quick Filter options, where you can filter the data using the filterable fields, there is also a free form text box, where you can enter text and filter the table.

- All—Displays all alarms.
- Manage Preset Filter—Displays any previously saved filters and allows you to edit and delete previously saved filters.
- Assigned to Me—Displays all alarms assigned to you.
- Unassigned Alarms—Displays all unassigned alarms.
- Alarms in Last 5 Minutes
- Alarms in Last 15 Minutes
- Alarms in Last 30 Minutes
- Alarms in the last hour
- Alarms in the last 8 hours
- Alarms in the last 24 hours
- Alarms in last 7 days
- All wired alarms—Displays all alarms for wired devices.
- All wireless alarms—Displays all alarms for wireless devices.

Viewing Alarm Details

You can view alarm details from the **Monitor > Alarms** page by clicking the expand icon to the far left of the **Monitor > Alarms** page for the alarm for which you want to see details. The details that are displayed depend on the alarm type you selected.

Table 5-60 Viewing Alarm Details

Section	Field	Description
General Info[1]	Failure Source	Indicates the source of the event (including name and/or MAC address).
	Owner	Name of person to which this alarm is assigned, or blank.
	Acknowledged	Displays whether or not the alarm is acknowledged by the user.
	Category	The category of the alarm (for example, AP, Rogue AP, or Security).
	Created	Month, day, year, hour, minute, second, AM or PM alarm created.
	Modified	Month, day, year, hour, minute, second, AM or PM alarm last modified.
	Generated By	Device that generated the alarm.
	Severity	Level of security: Critical, Major, Minor, Warning, Clear, Info.
	Previous Severity	The severity of the alarm the after the most recent polling cycle.

Table 5-60 Viewing Alarm Details

Section	Field	Description
Device Info	Device Name	Name of the device.
	Device Address	IP address of the device.
	Device Contact	Contact information for the device.
	Device Location	Location of the device.
	Device Status	Status of the device.
Messages		Device information retrieved from log messages.
Annotation		Lists current notes regarding this rogue access point. To add a new note, click **New Annotation**. Type the note and click **Post** to save and display the note or **Cancel** to close the page without saving the note.

[1] The General information may vary depending on the type of alarm. For example, some alarm details may include location and switch port tracing information.

From the Alarms list page, you can also view the events for the alarm you selected as explained in Viewing Events Related to Alarms, page 5-129.

Viewing Events Related to Alarms

When you select **Monitor > Alarms** page, you can view alarm summary information by hovering your mouse over an alarm severity in the Severity column and clicking the icon that appears.

A dialog appears displaying the top 5 events related to the alarm you selected.

Click **Events** to display *all* events associated with the selected alarm.

Modifying Alarms

From the **Monitor > Alarms** page, you can modify the alarms by selecting the checkbox next to an alarm and then clicking one of the tasks at the top of the Alarm Browser page:

Note The alarms that appear on the Monitor > Alarms page depend on the settings you specify on the Administration > Settings page. See Modifying Alarm Settings, page 5-132 for more information.

- Change Status—Change the alarm status to one of the following:
  - Acknowledge—You can acknowledge the alarm. By default, acknowledged alarms are not displayed in the Alarm Browser page. Acknowledged alarms remain in NCS and you can search for all acknowledged alarms using the alarm search functionality. See "Acknowledging Alarms" for more information.
  - Unacknowledge—You can choose to unacknowledge an already acknowledged alarm.
  - Clear—Clear the selected alarm(s). The alarm is removed from the Alarm Browser. Cleared alarms remain in NCS and you can search for all cleared alarms using the alarm search functionality

Note Once the severity is Clear, the alarm is deleted from NCS after 30 days by default. You can modify this setting on the Administration > Settings page.

- Assign—For the selected alarm, you can
  - Assign to me—Assigns the alarm to the specified user.
  - Unassign—Removes the specified owner from the alarm.
- Annotation—Enter an annotation for the selected alarm, then click **Post**. The annotation you entered appears when you view the alarm details.
- Delete—Delete the selected alarm(s). Indicates that the alarm is no longer detected by any device.

Specifying Email Notifications for Alarms

From the **Monitor > Alarms** page, you can set up email notifications for alarms based on the alarm category and severity level.

Step 1 Choose **Monitor > Alarms**, then click **Email Notification**.

Step 2 Select the Enable checkbox next to the alarm category for which you want to set up email notifications, then click **Save**.

NCS will send email notifications when alarms for the categories you specified occur.

Modifying the Alarm Browser

Choose **Monitor > Alarms** to view a list of alarms. You can also click **Alarm Browser** in the toolbar at the bottom of the NCS page. You can modify the following information displayed in the Alarm Browser:

- To reorder the columns, drag and drop the column headings into any position.
- Click on a column heading to sort the information by that column. By default, the column is sorted in descending order. Click the column heading again to change the sort the column in ascending order.

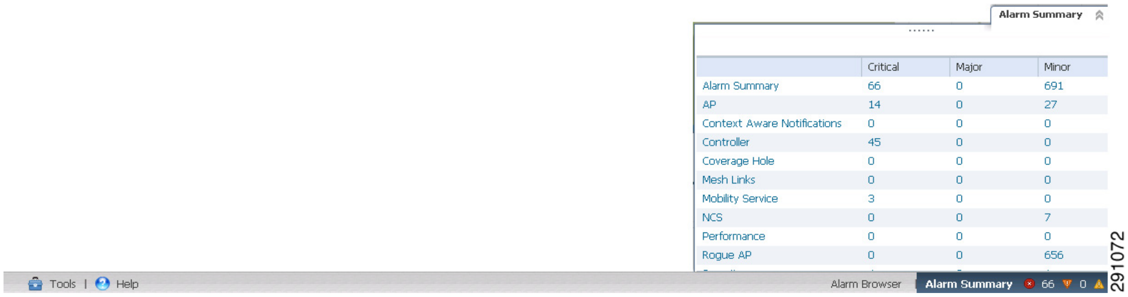
Note Not every column is sortable. Hover your mouse cursor over a column heading, and NCS will display whether the column is sortable.

- To customize which columns are displayed, click the Settings icon, then click **Columns**. Select the checkbox next to columns you want to appear, and unselect the boxes for the columns you do not want to appear in the Alarm Browser window.

Viewing the Alarm Summary

When NCS receives an alarm message from a controller, switch, or NCS, it displays an alarm indicator in the Alarm Summary. The Alarm Summary is at the bottom of the NCS page and displays the total count of critical, major, and minor alarms currently detected by NCS. Hover your mouse cursor over the Alarm Summary, and the alarm details are displayed as shown in Figure 5-6.

Figure 5-6 NCS Alarm Summary



Alarm Summary

	Critical	Major	Minor
Alarm Summary	66	0	691
AP	14	0	27
Context Aware Notifications	0	0	0
Controller	45	0	0
Coverage Hole	0	0	0
Mesh Links	0	0	0
Mobility Service	3	0	0
NCS	0	0	7
Performance	0	0	0
Rogue AP	0	0	656

Note The alarms that appear on the Alarm Summary and on the Monitor > Alarms page depends on the settings you specify on the Administration > Settings page. By default, acknowledged alarms are not shown.See Modifying Alarm Settings, page 5-132 for more information.

Alarms are color coded as follows:

- Red—Critical Alarm
- Orange—Major Alarm
- Yellow—Minor Alarm

Alarms indicate the current fault or state of an element, and alarms are usually generated by one or more events. The alarm can be cleared but the event remains. See Alarms and Events Overview for more information about alarms.

Note By default, alarm counts refresh every minute. You can modify when alarms are refreshed on the Administration > User Preferences page.

When you hover your mouse cursor over the Alarm Summary, a window appears listing the number of critical, major, and minor alarms for each of alarm category. You can specify which alarm categories are displayed in the Alarm Summary on the Administration > User Preferences page. By default, all categories are displayed:

- Alarm Summary—Displays a summary of the total alarms for all alarm categories.
- AP—Display counts for AP alarms such as AP Disassociated from controller, Thresholds violation for Load, Noise or Interference, AP Contained as Rogue, AP Authorization Failure, AP regulatory domain mismatch, or Radio card Failure.
- Context Aware Notifications
- Controller—Displays counts for controller alarms, such as reachability problems from NCS and other controller failures (fan failure, POE controller failure, AP license expired, link down, temperature sensor failure, and low temperature sensed).
- Coverage Hole—Displays counts for coverage hole alarms generated for access points whose clients are not having enough coverage set by thresholds. See the "Monitoring Maps" for more information.
- Mesh Links—Displays counts for mesh link alarms, such as poor SNR, console login, excessive parent change, authorization failure, or excessive association failure.
- Mobility Services—Displays counts for location alarms such as reachability problems from NCS and location notifications (In/Out Area, Movement from Marker, or Battery Level).

- NCS—Displays counts for NCS alarms.
- Performance—Displays counts for performance alarms.
- Rogue AP—Displays counts for malicious rogue access points alarms.
- Rogue Adhoc—Displays counts for unclassified rogue access point alarms.
- Security—Displays counts for security alarms such as Signature Attacks, AP Threats/Attacks, and Client Security Events.
- Switch—Displays counts for switch alarms such as authentication errors.

Modifying Alarm Settings

You can modify the following settings for alarms:

- Alarm count refresh rate—See Modifying Alarm Count Refresh Rate
- Alarm severity levels—See Configuring Alarm Severity Levels

Modifying Alarm Count Refresh Rate

By default, alarm counts refresh every minute. You can modify the refresh rate by selecting **Administration > User Preferences**, and then selecting a new value for the Refresh Alarm Count in the Alarm Summary Every menu.

Configuring Alarm Severity Levels

The Administration > Settings > Severity Configuration page allows you to change the severity level for newly generated alarms.

Note Existing alarms remain unchanged.

To reconfigure the severity level for a newly generated alarm, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, select **Severity Configuration**.

Step 3 Select the check box of the alarm condition whose severity level you want to change.

Step 4 From the Configure Security Level drop-down list, select from the following severity levels:

- Critical
- Major
- Minor
- Warning
- Informational
- Reset to Default

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the change or **Cancel** to leave the security level unchanged.

Working with Alarms

You can view, assign, and clear alarms and events on access points and mobility services engine using NCS.

This section also describes on how to have email notifications of alarms sent to you.

- Assigning and Unassigning Alarms
- Deleting and Clearing Alarms
- Acknowledging Alarms

Assigning and Unassigning Alarms

To assign and unassign an alarm to yourself, follow these steps:

Step 1 Perform an advanced search for access point alarms. See "Advanced Search" for more information.

Step 2 Select the alarms that you want to assign to yourself by selecting their corresponding check boxes.

Note To unassign an alarm assigned to you, Unselect the box next to the appropriate alarm. You cannot unassign alarms assigned to others.

Step 3 From the Select a command drop-down list, choose **Assign to Me** (or **Unassign**) and click **Go**.

If you choose Assign to Me, your username appears in the Owner column. If you choose Unassign, the username column becomes empty.

Deleting and Clearing Alarms

To delete or clear an alarm from a mobility services engine, follow these steps:

Step 1 From the **Monitor** > **Alarms** page, select the alarms that you want to delete or clear by selecting their corresponding check boxes.

Note If you delete an alarm, NCS removes it from its database. If you clear an alarm, it remains in the NCS database, but in the Clear state. You clear an alarm when the condition that caused it no longer exists.

Step 2 From the Select a command drop-down list, choose **Delete** or **Clear**, and click **Go**.

Note To set up cleanup of old alarms and cleared alarms, choose **Administration > Settings > Alarms**. See "Configuring Alarms" for more information.

Acknowledging Alarms

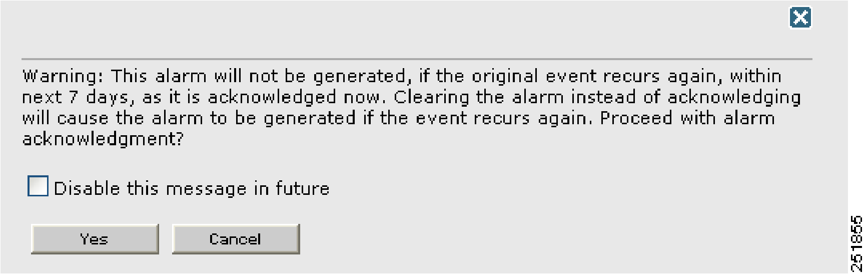
You may want certain alarms to be removed from the Alarms List. For example, if you are continuously receiving an interference alarm from a certain access point on the 802.11g interface, you may want to stop that access point from being counted as an active alarm on the Alarm Summary page or any alarms list. In this scenario, you can find the alarm for the 802.11g interface in the Alarms list, select the check box, and choose **Acknowledge** from the Select a command drop-down list.

Now if the access point generates a new violation on the same interface, NCS will not create a new alarm, and the Alarm Summary page shows no new alarms. However, if the interference violation is created on another interface, such as 802.11a, a new alarm is created.

By default, acknowledged alarms are not displayed in either the Alarm Summary page or any alarm list page. Also, no emails are generated for these alarms after you have marked them as acknowledged. By default, acknowledged alarms are not included for any search criteria. To change this default, go to the **Administration** > **Settings** > **Alarms** page and disable the **Hide Acknowledged Alarms** preference.

When you acknowledge an alarm, the following warning appears as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled (see Figure 5-7).

Figure 5-7 Alarm Warning



Warning: This alarm will not be generated, if the original event recurs again, within next 7 days, as it is acknowledged now. Clearing the alarm instead of acknowledging will cause the alarm to be generated if the event recurs again. Proceed with alarm acknowledgment?

☐ Disable this message in future

Note When you acknowledge an alarm, a warning displays as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled. Use the **Administration** > **User Preferences** page to disable this warning message.

You can also search for all previously acknowledged alarms to reveal the alarms that were acknowledged during the last seven days. NCS automatically deletes cleared alerts that are more than seven days old so your results can only show activity for the last seven days. Until an existing alarm is deleted, a new alarm cannot be generated for any managed entity for which NCS has already generated an alarm.

Monitoring Access Point Alarms

The Access Point Alarms page displays the access point based alarms on your network.

To access the AP alarms page, do one of the following:

- Perform a search for AP alarms. See "Using the Search Feature" for more information.
- Click the Access Point number link in the Alarm Summary box.

The Monitor AP Alarms page contains the following parameters:

- Severity—Indicates the severity of the alarm including:

Icon	Meaning
⊗	Critical
▼	Major
⚠	Minor
◆	Warning
ℹ	Info
?	Unknown **Note** When the controller goes down, the controller inventory dashlet shown the controller status as critical. But the radio inventory dashlet, will retain the last known status. In Monitor > AP page, the AP alarm status is shown as "Unknown".
✓	Clear—Displays if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from NCS after 30 days.

- Failure Source—Device that generated the alarm.
- Owner—Name of the person to which this alarm is assigned, or blank.
- Date/Time—The time at which the alarm was generated.
- Message—The associated message displayed in the NCS alarm browser.
- Category—Indicates the category assigned to the alarm such as rogue AP, controller, switch, and security.
- Condition—Condition that caused the alarm.
- Acknowledged—Displays whether or not the alarm is acknowledged by the user. See "Acknowledging Alarms" for more information.

Monitoring Air Quality Alarms

The Air Quality Alarms page displays air quality alarms on your network.

To access the air quality alarms page, do one of the following:

- Perform a search for Performance alarms. See "Using the Search Feature" for more information.
- Click the Performance number link in the Alarm Summary box.

The Monitor Air Quality Alarms page contains the following parameters:

- Severity—Indicates the severity of the alarm including:

Icon	Meaning
⊗	Critical
▽	Major
⚠	Minor
◆	Warning
ⓘ	Info
☑	Clear—Displays if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from NCS after 30 days.

- Failure Source—Device that generated the alarm.
- Owner—Name of the person to which this alarm is assigned, or blank.
- Date/Time—The time at which the alarm was generated.
- Message—The associated message displayed in the NCS alarm browser.
- Acknowledged—Displays whether or not the alarm is acknowledged by the user. See "Acknowledging Alarms" for more information.

Select a command Menu

Select one or more alarms by selecting their respective check boxes, select one of the following commands from the Select a command drop-down list, and click **Go**.

- Assign to me—Assign the selected alarm(s) to the current user.
- Unassign—Unassign the selected alarm(s).
- Clear—Clear the selected alarm(s).
- Delete—Delete the selected alarm(s).
- Acknowledge—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See "Acknowledging Alarms" for more information.

Note The alarm remains in NCS and you can search for all Acknowledged alarms using the alarm search functionality.

- Unacknowledge—Unacknowledge an already acknowledged alarm.
- Email Notification—Takes you to the **All Alarms** > **Email Notification** page to view and configure email notifications. See "Monitoring RFID Tags" for more information.

Monitoring CleanAir Security Alarms

The CleanAir Security Alarms page displays security alarms on your network.

To access the security alarms page, do one of the following:

- Perform a search for Security alarms. See "Using the Search Feature" for more information.
- Click the Security number link in the Alarm Summary box.

The Monitor CleanAir Security Alarms page contains the following parameters:

- Severity—Indicates the severity of the alarm including:

Icon	Meaning
⊗	Critical
▽	Major
⚠	Minor
◆	Warning
ⓘ	Info
✓	Clear—Displays if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from NCS after 30 days.

- Failure Source—Device that generated the alarm.
- Owner—Name of the person to which this alarm is assigned, or blank.
- Date/Time—The time at which the alarm was generated.
- Message—The associated message displayed in the NCS alarm browser.
- Acknowledged—Displays whether or not the alarm is acknowledged by the user. See "Acknowledging Alarms" for more information.

Select a command Menu

Select one or more alarms by selecting their respective check boxes, select one of the following commands from the Select a command drop-down list, and click **Go**.

- Assign to me—Assign the selected alarm(s) to the current user.
- Unassign—Unassign the selected alarm(s).
- Clear—Clear the selected alarm(s).
- Delete—Delete the selected alarm(s).
- Acknowledge—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See "Acknowledging Alarms" for more information.

Note The alarm remains in NCS and you can search for all Acknowledged alarms using the alarm search functionality.

- Unacknowledge—Unacknowledge an already acknowledged alarm.
- Email Notification—Takes you to the **All Alarms** > **Email Notification** page to view and configure email notifications. See "Monitoring RFID Tags" for more information.

Monitoring Email Notifications

The Cisco NCS includes a built-in email notification function which can notify the network operator when critical alarms occur.

The email notification filter page allows you to add a filter for each alert category. Severity level is set to critical by default when the alert category is enabled, but you can choose a different severity level for different categories. Email notifications are generated only for the severity levels that are configured.

To configure e-mail notifications, follow these steps:

Step 1 Choose **Monitor > Alarms**.

Step 2 From the Select a command drop-down list, choose **Email Notification**.

Step 3 Click **Go**.

Step 4 Click an Alarm Category to edit severity level and e-mail recipients for its e-mail notifications.

Step 5 Select the severity level check box(es) (Critical, Major, Minor, or Warning) for which you want a notification sent.

Step 6 Enter the notification recipient e-mail addresses in the To text box.

Note Separate multiple e-mail addresses with a comma.

Step 7 Click **OK**.

Step 8 Select the **Enabled** check box for applicable alarm categories to activate the delivery of e-mail notifications.

Step 9 Click **OK**.

Monitoring Severity Configurations

You can change the severity level for newly generated alarms.

Note Existing alarms remain unchanged.

To change the severity level of newly-generated alarms, follow these steps:

Step 1 Choose **Administration > Setting**.

Step 2 Choose **Severity Configuration** from the left sidebar menu.

Step 3 Select the check box of the alarm condition for which you want to change the severity level.

Step 4 From the **Configure Severity Level** drop-down list, choose the new severity level (Critical, Major, Minor, Warning, Informational, Reset to Default).

Step 5 Click **Go**.

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

Monitoring Cisco Adaptive wIPS Alarms

Alarms from Cisco Adaptive wIPS DoS (Denial of Service) and security penetration attacks are classified as security alarms. You can view these wIPS alarms and their details in the **Monitor** > **Alarms** section of NCS.

To view a list of wIPs DoS and security penetration attack alarms, follow these steps:

Step 1 Perform a search for Security alarms using the Advanced Search feature. See "Advanced Search" for more information on performing an advanced search.

The following information is provided for wIPS alarms:

- Severity—Severity levels include critical, major, info, warning, and clear.
- Failure Object—Displays the name and IP or MAC address of the object for which the alarm was generated. Click the Failure Object to view alarm details. See "Monitoring Cisco Adaptive wIPS Alarm Details" for more information on viewing wIPS alarm details.
- Date/Time—Displays the date and time that the alarm occurred.
- Message—Displays a message explaining why the alarm occurred (such as the applicable wIPS policy).
- Acknowledged—Displays whether or not the alarm is acknowledged by the user.
- Category—Indicates the category of this alarm such as Security.
- Condition—Displays a description of what caused this alarm to be triggered.

When there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

To add, remove, or reorder columns in the table, click the **Edit View** link to go to the Edit View page.

Select a command

Using the **Select a command** drop-down list, you can perform the following actions on the selected alarms:

- Assign to me—Assign the selected alarm(s) to the current user.
- Unassign—Unassign the selected alarm(s).
- Delete—Delete the selected alarm(s).
- Clear—Clear the selected alarm(s).
- Acknowledge—You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in NCS and you can search for all Acknowledged alarms using the alarm search functionality.
- Unacknowledge—You can choose to unacknowledge an already acknowledged alarm.
- Email Notification—Takes you to the All **Alarms** > **Email Notification** page to view and configure email notifications.

To perform an action on the selected alarm, follow these steps:

Step 1 Select an alarm by selecting its check box.

Step 2 From the Select a command drop-down list, select a the applicable command.

Step 3 Click **Go**.

Monitoring Cisco Adaptive wIPS Alarm Details

Choose **Monitor > Alarms** > <*failure object*> to view details of the selected Cisco wIPS alarm. The following Alarm Details are provided for Cisco Adaptive wIPS alarms:

- General
  - Detected By wIPS AP—The access point that detected the alarm.
  - wIPS AP IP Address—The IP address of the wIPS access point.
  - Owner—Name of person to which this alarm is assigned or left blank.
  - Acknowledged—Displays whether or not the alarm is acknowledged by the user.
  - Category—For wIPS, the alarm category is Security.
  - Created—Month, day, year, hour, minute, second, AM or PM that the alarm was created.
  - Modified—Month, day, year, hour, minute, second, AM or PM that the alarm was last modified.
  - Generated By—Indicates how the alarm event was generated (either NMS or from a trap).

NMS (Network Management System - NCS)—Generated through polling. NCS periodically polls the controllers and generates events. NCS generates events when the traps are disabled or when the traps are lost for those events. In this case "Generated by" will be NMS

Trap—Generated by the controller. NCS process these traps and raises corresponding events for them. In this case "Generated by" will be Controller.

- Severity—Level of severity including critical, major, info, warning, and clear.
- Last Disappeared—The date and time that the potential attack last disappeared.
- Channel—The channel on which the potential attack occurred.
- Attacker Client/AP MAC—The MAC address of the client or access point that initiated the attack.
- Attacker Client/AP IP Address—The IP address of the client or access point that initiated the attack.
- Target Client/AP IP Address—The IP address of the client or access point targeted by the attacker.
- Controller IP Address—The IP address of the controller to which the access point is associated.
- MSE—The IP address of the associated mobility services engine.
- Controller MAC address—The MAC address of the controller to which the access point is associated.
- wIPS access point MAC address
- Forensic File
- Event History—Takes you to the "Monitoring Alarms" page to view all events for this alarm.

- Annotations—Enter any new notes in this box and click **Add** to update the alarm. Notes are displayed in the "Annotations" display area.
- Messages—Displays information about the alarm.
- Audit Report—Click to view config audit alarms details. This report is only available for Config Audit alarms.

  Configuration audit alarms are generated when audit discrepancies are enforced on config groups.

  Note If enforcement fails, a critical alarm is generated on the config group. If enforcement succeeds, a minor alarm is generated on the config group.
  The alarms have links to the audit report where you can view a list of discrepancies for each controller.

- Rogue Clients—If the failure object is a rogue access point, information about rogue clients is displayed.

Select a command

Select one or more alarms by selecting their respective check boxes, selecting one of the following commands, and clicking **Go**.

- Assign to me—Assign the selected alarm(s) to the current user.
- Unassign—Unassign the selected alarm(s).
- Delete—Delete the selected alarm(s).

- Clear—Clear the selected alarm(s).
- Acknowledge—You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in NCS and you can search for all Acknowledged alarms using the alarm search functionality.
- Unacknowledge—You can choose to unacknowledge an already acknowledged alarm.
- Email Notification—Takes you to the All **Alarms** > **Email Notification** page to view and configure email notifications.
- Event History—Takes you to the Monitor **Alarms** > **Events** page to view events for Rogue Alarms.

Monitoring Events

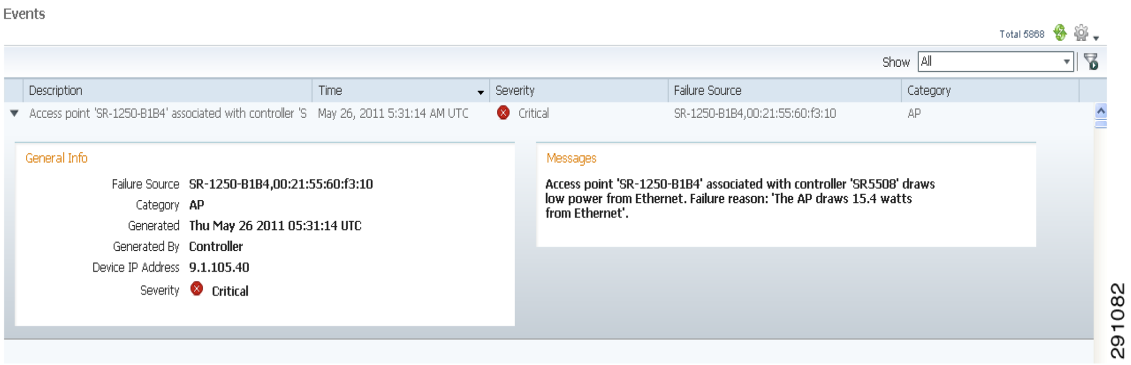
One or more events may generate an abnormal state or alarm. The alarm can be cleared, but the event remains. Choose **Monitor > Events** to access the Events page, which displays the following information:

- Description—Describes the event details.
- Time—Indicates the date and time the event was generated.
- Severity—Event severities include: Critical, Major, Minor, Warning, Cleared, or Information.
- Failure Source—Indicates the source of the event (including name and/or MAC address).
- Category—Type of event such as Rogue AP, Security, or AP

Click on any column heading to sort by that column.

Use the quickview icon to disclose more information on the event. The additional information for the event is divided into general information and the message. In the general information, the failure source, the category, severity, generated time and IP address. The message of the event is also displayed. (See Figure 5-8)

Figure 5-8 Viewing Events



Description	Time	Severity	Failure Source	Category
Access point 'SR-1250-B1B4' associated with controller 'S	May 26, 2011 5:31:14 AM UTC	⊗ Critical	SR-1250-B1B4,00:21:55:60:f3:10	AP

General Info

Failure Source SR-1250-B1B4,00:21:55:60:f3:10
Category AP
Generated Thu May 26 2011 05:31:14 UTC
Generated By Controller
Device IP Address 9.1.105.40
Severity ⊗ Critical

Messages

Access point 'SR-1250-B1B4' associated with controller 'SR5508' draws low power from Ethernet. Failure reason: 'The AP draws 15.4 watts from Ethernet'.

Note Events also has preset, quick and advanced filters similar to alarms. These filters work in same way as the filters in alarms.

When you filter the table using the Search feature, the Events page may display the additional information. See "Advanced Search"(Advanced Search results for Events) for more information on performing a search. The additional information includes:

- Coverage Hole Events
  - Access Point Name
  - Failed Clients—Number of clients that failed due to the coverage hole.
  - Total Clients—Total number of clients affected by the coverage hole.
  - Radio Type—The radio type (802.11b/g or 802.11a) of the applicable access point.
  - Coverage Threshold
- Rogue AP Events
  - Vendor—Rogue access point vendor name or Unknown.
  - Classification Type—Indicates the type of rogue access point including Malicious, Friendly, or Unclassified.
  - On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
  - Radio Type—Lists all radio types applicable to this rogue access point.
  - State—Indicates the state of the alarm. Possible states for adhoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
  - SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

Note See "Monitoring Rogue Alarm Events" or "Viewing Rogue AP Event Details" for more information on rogue access points events.

- Adhoc Rogue Events
  - Vendor—Rogue access point vendor name or Unknown.
  - On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
  - Radio Type—Lists all radio types applicable to this rogue access point.
  - State—Indicates the state of the alarm. Possible states for adhoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
  - SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Interference
  - Detected By—IP address of the device that detected the interference.
  - ID—ID of the device that detected the interference.
- Mesh Links

- Client
- Context Aware Notification
- Pre Coverage Hole
  - Client MAC Address—MAC address of the client affected by the Pre Coverage Hole.
  - AP MAC Address—MAC address of the applicable access point.
  - Radio Type—The radio type (802.11b/g or 802.11a) of the applicable access point.
  - Power Level—Access Point transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, 5 = 0.195 to 6.25% power).
  - Client Type—Client type can be laptop(0), pc(1), pda(2), dot11mobilephone(3), dualmodephone(4), wgb(5), scanner(6), tabletpc(7), printer(8), projector(9), videoconfsystem(10), camera(11), gamingsystem(12), dot11deskphone(13), cashregister(14), radiotag(15), rfidsensor(16), server(17)
  - WLAN Coverage Hole Status

If there is more than one page of events, the number of pages is displayed with a scroll arrow on each side. Use this to view additional events.

This section contains the following topics:

- Searching Events
- Monitoring Failure Objects
- Monitoring Events for Rogue APs
- Viewing Adhoc Rogue Event Details
- Monitoring Cisco Adaptive wIPS Events
- Monitoring Cisco Adaptive wIPS Events
- Working with Events

Searching Events

Use the NCS Search feature to find specific events or to create and save custom searches. See one of the following topics for additional information:

- Using the Search Feature
- Quick Search
- Advanced Search
- Saved Searches

Monitoring Failure Objects

Note The event categories Location Servers and Location Notifications appear only in the Cisco NCS Location version.

Choose **Monitor > Events**, then click the expand icon to the far left of the **Monitor > Events** page for the event for which you want to see details. Details about the event are displayed. Depending on the type of event you selected, the associated details will vary.

- General Info
  - Failure Source—Indicates the source of the event (including name and/or MAC address).
  - Category—Type of alarm such as Security or AP.
  - Generated—Date and time that the event was generated.
  - Generated By—Indicates how the alarm event was generated (either NMS or from a trap).

    NMS (Network Management System - NCS)—Generated through polling. NCS periodically polls the controllers and generates events. NCS generates events when the traps are disabled or when the traps are lost for those events. In this case "Generated by" will be NMS.

    Trap—Generated by the controller. NCS process these traps and raises corresponding events for them. In this case "Generated by" will be Controller.
  - Device IP Address—IP address of the alarm-generating device.
  - Severity—Level of severity including critical, major, info, warning, and clear.
- Messages—Message explaining why the event occurred.

Monitoring Events for Rogue APs

Choose **Monitor > Events**. From the left sidebar menu Event Category, choose **Rogue AP** to display the Monitoring Events page for rogue access points. Click an item under Rogue MAC Address to display this page.

This page displays alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by controllers. The following parameters appear:

General

- Rogue MAC Address
- Vendor
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Owner—Name of person to which this alarm is assigned, or (blank).
- State—State of this radio relative to the network or Port. Rogue access point radios appear as "Alert" when first scanned by the Port, or as "Pending" when operating system identification is still underway.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Containment Level—An access point which is being contained will either not be able to provide service at all, or will provide exceedingly slow service. There is a level associated with the containment activity which indicates how many Cisco 1000 Series lightweight access points to use in containing the threat. This service must be initiated and halted by the administrator. Containment Type - Contained if the rogue access point clients have been contained at Level 1 through Level 4 under Update Status, otherwise Unassigned.

- Channel—Indicates the band at which the adhoc rogue is broadcasting.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Created—Date and time that the event occurred.
- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
  - NMS (Network Management System - NCS)—Generated through polling. NCS periodically polls the controllers and generates events. NCS generates events when the traps are disabled or when the traps are lost for those events. In this case “Generated by” will be NMS.
  - Trap—Generated by the controller. NCS process these traps and raises corresponding events for them. In this case “Generated by” will be Controller.
- Device IP Address—IP address of the alarm-generating device.
- Severity—Level of severity, Critical, Major, Minor, Warning, Clear, Info. Color coded.

Message—Displays descriptive information about the alarm.

Help—Displays information about the alarm.

Note Use the Advance Search feature to find specific events. See Advanced Search for more information.

Monitoring Events for Adhoc Rogues

Choose **Monitor > Events**. From the left sidebar menu Event Category, choose **Adhoc Rogue** to display the Monitoring Events page for adhoc rogue. Click an item under Rogue MAC Address to display adhoc rogue event details.

General

- Rogue MAC Address
- Vendor
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Owner—Name of person to which this alarm is assigned, or (blank).
- State—State of this radio relative to the network or Port. Rogue access point radios appear as “Alert” when first scanned by the Port, or as “Pending” when operating system identification is still underway.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Containment Level—An access point which is being contained will either not be able to provide service at all, or will provide exceedingly slow service. There is a level associated with the containment activity which indicates how many Cisco 1000 Series lightweight access points to use in containing the threat. This service must be initiated and halted by the administrator. Containment Type - Contained if the rogue access point clients have been contained at Level 1 through Level 4 under Update Status, otherwise Unassigned.

- Channel—Indicates the band at which the adhoc rogue is broadcasting.
- Created—Date and time that the event occurred.
- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
  - NMS (Network Management System - NCS)—Generated through polling. NCS periodically polls the controllers and generates events. NCS generates events when the traps are disabled or when the traps are lost for those events. In this case "Generated by" will be NMS.
  - Trap—Generated by the controller. NCS process these traps and raises corresponding events for them. In this case "Generated by" will be Controller.
- Device IP Address—IP address of the alarm-generating device.
- Severity—Level of severity, Critical, Major, Minor, Warning, Clear, Info. Color coded.

Message—Displays descriptive information about the alarm.

Help—Displays information about the alarm.

Monitoring Cisco Adaptive wIPS Events

Choose **Monitor > Events** to view wIPS events. One or more events may generate an abnormal state or alarm. The alarm can be cleared, but the event remains. For more information regarding monitoring events, see "Monitoring Events."

The following sections provide additional information regarding Cisco Adaptive wIPS:

- Configuring wIPS Profiles
- NCS Services
- wIPS Policy Alarm Encyclopedia

Perform an events search to narrow the results to mobility services engine or Security events only. To view mobility services engine or Security events only, follow these steps:

Step 1 Choose **Monitor > Events**.

Step 2 From the left sidebar menu, choose **Mobility Service** or **Security** from the Event Category drop-down list.

Step 3 Click **Go**.

Note If there is more than one page of events, the number of pages is displayed with a scroll arrow on each side. Use this to view additional events.

Monitoring CleanAir Air Quality Events

You can use NCS to view the events generated on the air quality of the wireless network.

To view air quality events, follow these steps:

Step 1 Click Advanced Search in the NCS window.

The New Search page appears.

Step 2 In the New Search page, choose Events from the Search Category drop-down list.

Step 3 From the Severity drop-down list, choose the type of severity you want to search the air quality events.

Step 4 From the Event Category drop-down list, choose Performance.

Step 5 Click Go.

The air quality events page displays the following information:

- Severity—Indicates the severity of the alarm including:

Icon	Meaning
⊗	Critical
▼	Major
⚠	Minor
◆	Warning
ℹ	Info
✓	Clear—Displays if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from NCS after 30 days.

- Failure Source—Device that generated the alarm.
- Date/Time—The time at which the alarm was generated.

Viewing Air Quality Event Details

To view air quality event details, follow these steps:

Step 1 From the Air Quality Events page, click an item under Failure Source to access the alarm details page. See Monitoring CleanAir Air Quality Events.

Step 2 The air quality event page displays the following information:

- Failure Source—Device that generated the alarm.
- Category—The category this event comes under. In this case, Performance.
- Created—The time stamp at which the event was generated.
- Generated by—The device that generated the event.
- Device IP Address—The IP address of the device that generated the event.

- Severity—The severity of the event.
- Alarm Details—A link to the related alarms associated with this event. Click the link to know more about the alarm details.
- Message—Describes the air quality index on this access point.

Monitoring Interferer Security Risk Events

You can use NCS to view the security events generated on your wireless network.

To view interferer security events, follow these steps:

Step 1 Click **Advanced Search** in the NCS window.

The New Search page appears.

Step 2 In the New Search page, choose **Events** from the Search Category drop-down list.

Step 3 From the Severity drop-down list, choose the type of severity you want to search the air quality events.

Step 4 From the Event Category drop-down list, choose **Security**.

Step 5 Click **Go**.

The interferer security events page displays the following information:

- Severity—Indicates the severity of the alarm including:

Icon	Meaning
✖	Critical
▽	Major
⚠	Minor
◆	Warning
ℹ	Info
✓	Clear—Displays if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from NCS after 30 days.

- Failure Source—Device that generated the alarm.
- Date/Time—The time at which the alarm was generated.

Viewing Interferer Security Risk Event Details

To view interferer security event details, follow these steps:

Step 1 In the Interferer Security Event details page, click an item under Failure Source to access the alarm details page. See Monitoring Interferer Security Risk Events.

Step 2 The air quality event page displays the following information:

- Failure Source—Device that generated the alarm.
- Category—The category this event comes under. In this case, Security.
- Created—The time stamp at which the event was generated.
- Generated by—The device that generated the event.
- Device IP Address—The IP address of the device that generated the event.
- Severity—The severity of the event.
- Alarm Details—A link to the related alarms associated with this event. Click the link to know more about the alarm details.
- Message—Describes the interferer device affecting the access point.

Monitoring Health Monitor Events

You can use NCS to view the events generated by the Health Monitor.

To view the health monitor events, follow these steps:

Step 1 Click Advanced Search in the NCS window.

The New Search page appears.

Step 2 In the New Search page, choose Events from the Search Category drop-down list.

Step 3 From the Severity drop-down list, choose the type of severity you want to search the health monitor events.

Step 4 From the Event Category drop-down list, choose NCS.

Step 5 Click Go.

The health monitor events page displays the following information:

- Severity—Indicates the severity of the alarm including:

Icon	Meaning
⊗	Critical
▽	Major
⚠	Minor
◆	Warning

Icon	Meaning
ℹ	Info
✓	Clear

- Failure Source—Device that generated the alarm.
- Date/Time—The time at which the alarm was generated.
- Message—Describes the health details.

Viewing Health Monitor Event Details

To view health monitor event details, follow these steps:

Step 1 From the Health Monitor Events page, click an item under Failure Source to access the alarm details page. See the "Monitoring Health Monitor Events" section on page 5-150.

Step 2 The health monitor event page displays the following information:

- Failure Source—Device that generated the alarm.
- Category—The category this event comes under. In this case, NCS.
- Created—The time stamp at which the event was generated.
- Generated by—The device that generated the event.
- Device IP Address—The IP address of the device that generated the event.
- Severity—The severity of the event.
- Alarm Details—A link to the related alarms associated with this event. Click the link to know more about the alarm details.
- Message—Describes the event through a message.

Working with Events

You can use NCS to view mobility services engine and access point events. You can search and display events based on their severity (critical, major, minor, warning, clear, info) and event category or you can search for a mobility services engine and access point by its IP address, MAC address or name.

A successful event search displays the event severity, failure object, date and time of the event, and any messages for each event.

To display events, follow these steps:

Step 1 In Cisco NCS, click **Monitor > Events**.

Step 2 In the Events page:

- If you want to display the events for a specific element and you know its IP address, MAC address, or Name, enter that value in the Quick Search text box (left pane). Click **Go**.

- To display events by severity and category, select the appropriate options from the Severity and Event Category drop-down lists (left pane). Click **Search**.

Step 3 If NCS finds events that match the search criteria, it displays a list of these events.

Note For more information about an event, click the failure object associated with the event. Additionally, you can sort the events summary by each of the column headings.

Monitoring Site Maps

Maps provide a summary view of all your managed systems on campuses, buildings, outdoor areas, and floors. With the NCS database, you can add maps and view your managed system on realistic campus, building, and floor maps. See Monitoring Maps, page 6-1 for more information.

Monitoring Google Earth Maps

You can enable location presence by mobility server to provide expanded Civic (city, state, postal code, country) and GEO (longitude, latitude) location information beyond the Cisco default setting (campus, building, floor, and X, Y coordinates). This information can then be requested by clients on a demand basis for use by location-based services and applications. Location Presence can be configured when a new campus, building, floor, or outdoor area is being added or configured at a later date. See Monitoring Google Earth Maps, page 6-111 for more information.