JUNIPER NETWORKS

Junos® Space

Network Director Monitor Mode User Guide

Release
1.5

Published: 2013-10-15

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® Space Network Director Monitor Mode User Guide
1.5

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Documentation Conventions

Table 1 on page xii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub <default-metric** *metric***>;**

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to **techpubs-comments@juniper.net**, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

Monitor Mode Overview

Understanding Monitor Mode in Network Director

Monitor mode in Network Director provides you visibility into your network status and performance. Network Director monitors its managed devices and maintains the information it collects from the devices in a database. Monitor mode displays this information in easy-to-understand graphs and in tables that you can sort and filter, allowing you to quickly visualize the state of your network, spot trends developing over time, and find important details.

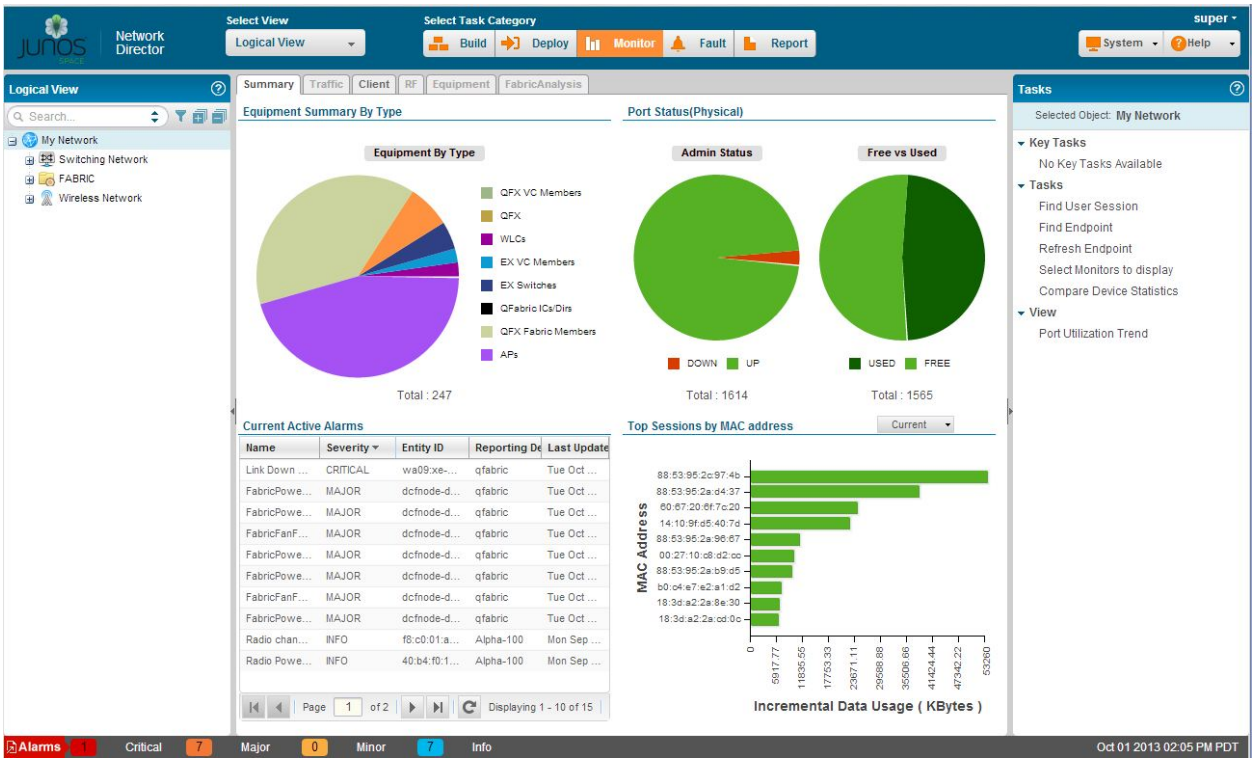
NOTE: **Monitor mode for the virtual view displays information specific to the virtual networks, virtual switches, and hosts. To know more about Monitor mode for virtual view, see** "Using Monitor Mode for Virtual Devices" on page 69.

Monitor mode divides monitoring activity into the following categories:

- Traffic—Provides information about traffic about switches, wireless LAN controllers, and interfaces.
- Client—Provides session information about clients connected to wireless access points and to 802.1X authenticator switch ports.
- RF—Provides information about the wireless environment and signal performance.
- Equipment—Provides information about the state of switches, wireless LAN controllers, interfaces, wireless access points, and radios.
- Fabric Analysis—Displays the results of running the Run Fabric Analyzer task on a QFabric device. It shows information about the health, connectivity, and topology of the QFabric.

You can access these categories through tabs on the Monitor mode landing page, as shown in Figure 1 on page 4. An additional tab, the Summary tab, is available that provides a high-level dashboard for the scope selected in the View pane. The monitoring information displayed in the Summary tab also appears on other tabs.

Figure 1: Monitor Mode Landing Page and Tabs



This topic describes:

Scope and Monitor Tab Availability

Your current scope—that is, your view and node selection in the View pane—affects which Monitor tabs are available. For example, if you select a switch, the RF tab is not available.

The shading of the tabs indicate whether a tab is selected, available, or not available:

- The currently selected tab has dark text on a light background.
- Tabs that are available but not selected have dark text on a dark background.
- Tabs that are not available for your current scope have light text on a light background.

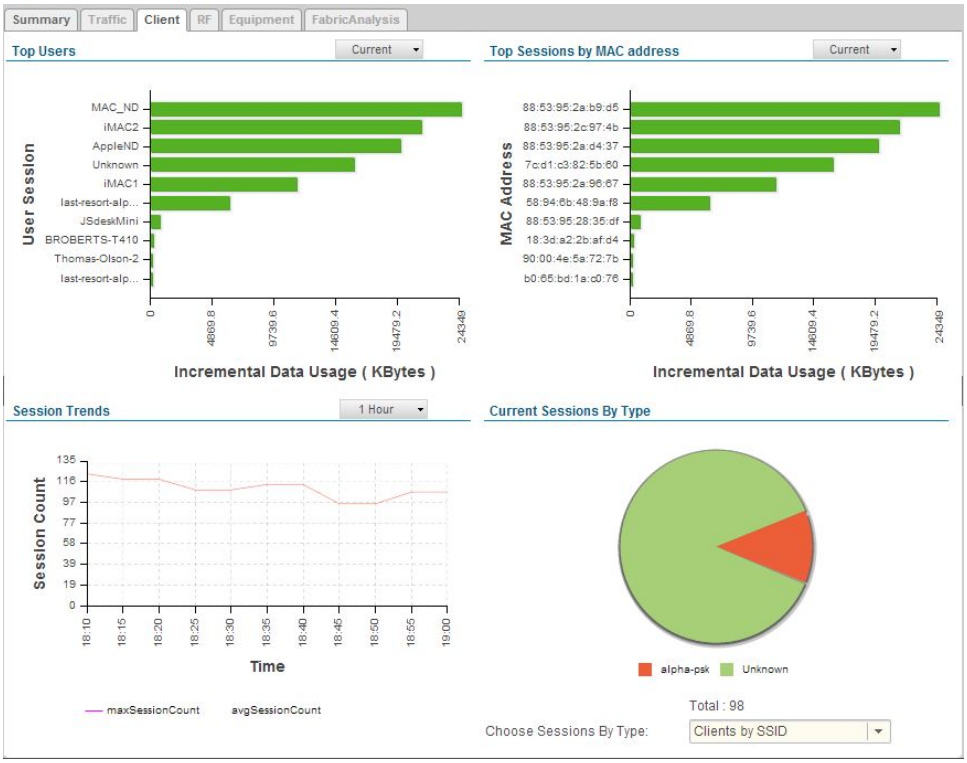
When you enter Monitor mode from another mode, the Summary tab is selected for all scopes. If you have selected a tab and then change scope, the tab remains selected if it

is supported in the new scope. If it is not supported in the new scope, Network Director selects a default tab for that scope.

Monitors and Tasks

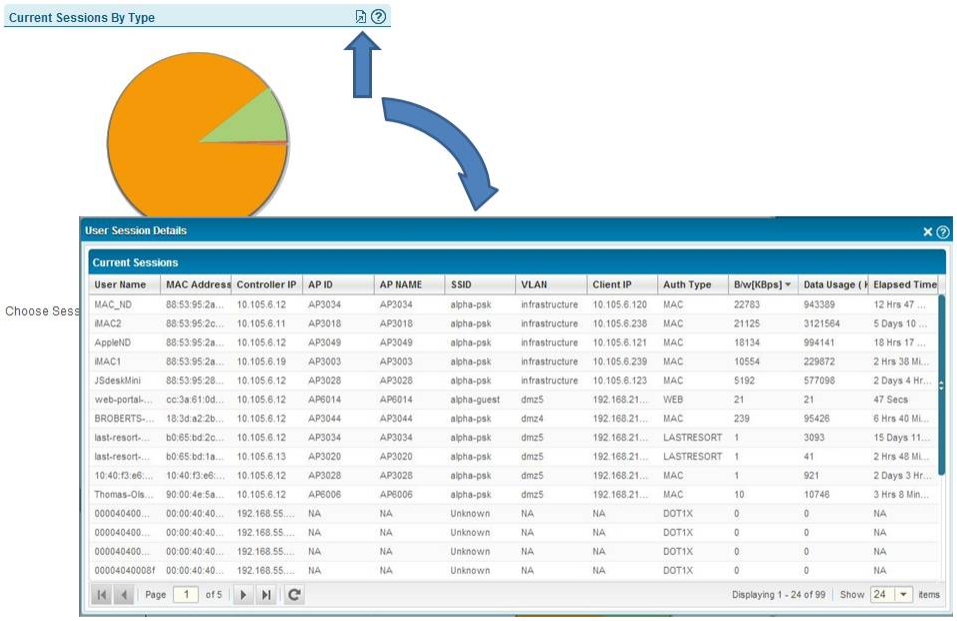
When you click a Monitor tab, the landing page for that tab is displayed, which contains a set of monitors. These monitor enable you to see at a glance important information about the aspect of your network being monitored. For example, the monitors in the Client tab, shown in Figure 2 on page 5, present high-level information about the sessions in the selected scope: the users and client sessions consuming the most bandwidth, the current count of active sessions, and the trend in session count over time.

Figure 2: The Client Tab Monitors



Detailed information is also available from many monitors when you click the Details icon on the monitor. If the Details icon is not visible in the title bar of a monitor, mouse over the monitor to make it visible. For example, if you click the Details icon from the Current Sessions By Type monitor, you can view detailed information about the current sessions, as shown in Figure 3 on page 6.

Figure 3: Accessing Session Details from the Current Session by Type Monitor



In addition to monitors, each tab provides a set of tasks available from the Tasks pane. These tasks enable you to perform additional monitoring functions. Some tasks enable you to view more specialized monitoring data; others enable you to perform an operation, such as pinging a host. For a complete list of tasks available in Monitor mode, see "Understanding the Monitor Mode Tasks Pane" on page 11.

The scope you select affects which monitors are displayed and which tasks are available. In the Equipment tab, for example, you see a different set of monitors for an EX Series switches than you see for Wireless LAN controllers.

Scope and Data Aggregation

Network Director enables you to more than monitor individual devices. It provides a broader network view by aggregating data from devices and making that data available for viewing at higher scopes within the network.

A good example is RF interference data. Network Director associates RF interference data with the radio that reported it. You can select a radio in the View pane to view the interference data reported by that radio. However, you can also view the RF interference data for the entire wireless network or for a particular location (floor, building or site). At each of these scopes, Network Director combines or aggregates the data associated with all the radios included in that scope.

Not all data is aggregated at higher scopes. For example, it does not make sense to provide power supply status at any higher scope than the device itself. Whenever monitors

are available at a scope higher than the device scope, however, the data presented is aggregated data from all devices contained in that scope.

How Network Director Collects and Displays Monitoring Data

Network Director collects monitoring data from all its managed devices at regular intervals known as polling intervals. These polling intervals can vary according to the type of data being collected. Network Director sets default polling intervals for each type of data—you can, however, change these polling intervals in Preferences.

The polling intervals are aligned to clock time. For example, if the polling interval is set to 5 minutes, then within every hour, Network Director collects data at :00, :05, :10, :15, and so on. If the polling interval is set to 15 minutes, Network Director collects data within every hour at :00, :15, :30, and :45.

Network Director uses the Juniper Networks Device Management Interface (DMI) to the managed devices to collect the data. If you have a Junos Space fabric, Network Director balances the load of polling the managed devices across the nodes in the fabric.

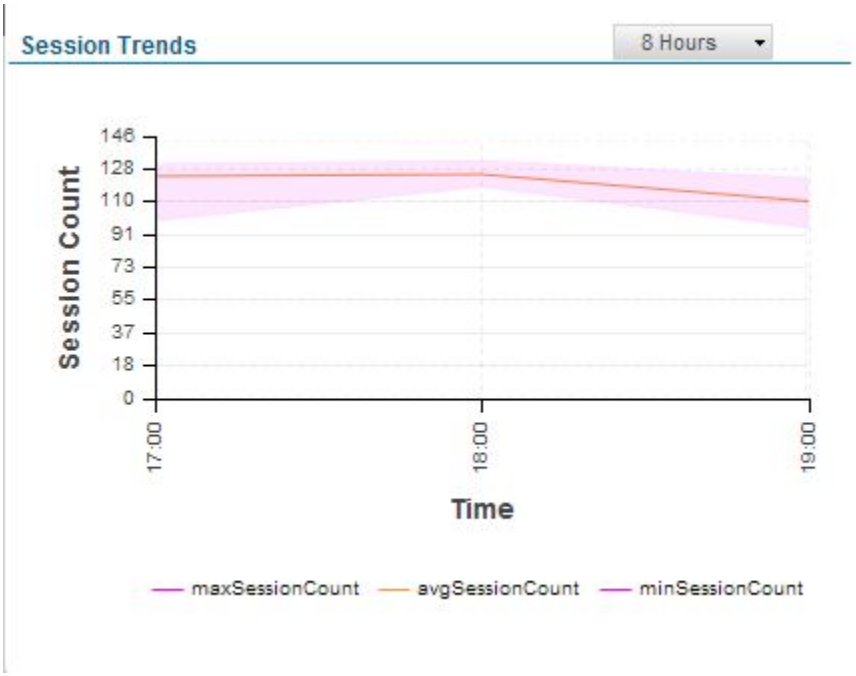
When you display a monitor, the current data is from the last polling interval. Displaying or refreshing a monitor does not trigger Network Director to collect data. However, Network Director automatically refreshes monitors with new data after a polling interval completes. Each monitor displays the time that the data was last refreshed.

The detail windows for monitors are not automatically refreshed after a polling period completes. You must manually refresh them to obtain new polling data.

How Network Director Displays and Stores Trend Data

In addition to displaying current data, Network Director also displays historical data so that you can view trends in network performance over time. Figure 4 on page 8 shows an example of trend graph.

Figure 4: Trend Graph Showing Change in Session Count in the Last 8 Hours



ERROR: Unresolved graphic fileref="" not found in "//cmsxml/default/main/supplemental/STAGING/images/".

When you display a trend graph, you can select the time period over which the data is displayed—usually 1 hour, 8 hours, 1 day, 1 week, 1 month, 3 months, 6 months, or 1 year. These predefined periods are always relative to the current time and date—that is, if you select a week, the data is from the last 7 days. You can also define a custom time period, which enables you to display data for a period between specific dates and times.

For a trend graph displaying a predefined period of 1 hour, the number of data points depends on the configured polling interval. For periods greater than an hour, the number of data points displayed depends on the time period selected and how Network Director consolidates data over time.

To allow storing of monitoring data for a long period of time, Network Director consolidates older data. Consolidation involves deriving a single value from a set of shorter term values, generally by averaging the shorter term values, and then using that value as a data point in a longer term data set. After the shorter term data is consolidated into longer term data, it is discarded to save storage space. For example, if a value is polled every 5 minutes, the set of 12 values is consolidated into a single value after an hour has passed. That value then becomes one of the 24 data points that makes up the data set for a day. Similarly, after a day has passed, data is consolidated into one data point that represents that day; after a month has passed, data is consolidated into a one data point that represents that month. Data is not kept longer than a year. You can, however, run reports on some monitoring data in Report Mode and archive the reports to maintain a history that is longer than a year.

Because of data consolidation, longer-term data is less granular than shorter-term data. However, for some kinds of data, Network Director also keeps track of the highest and lowest values within a data set. When you display longer-term data set, the graph contains shaded areas, as shown in Figure 4 on page 8, that indicate the high water mark and low water mark for the time period represented by the data point.

For all trend graphs, Network Director will not display data until it has more than two data points to display. This means that after you discover a device, trend data will not appear until three polling periods have passed.

More About the Monitor Tabs

The following sections provide more information about each tab in Monitor mode.

The Summary Tab

The Summary tab is displayed whenever you enter Monitor mode. It serves as a high-level dashboard for the current selected scope in the View pane.

The monitors displayed in the Summary tab can belong to any of the Monitor categories. Each scope has a predefined set of monitors that are displayed. For example, if your scope is the Wireless Network, a set of four monitors summarize the status of wireless equipment in the network, the interference sources in the network, the alarms active on the wireless devices, and the number of sessions in the wireless network.

When you select an individual device in the View pane, the Summary tab itself displays an arrow that indicates whether the device is up (green up arrow) or down (red down arrow).

For the My Network scope, you can customize what monitors appear on Summary tab, giving you the ability to view at a glance those aspects of network health and performance that are most important to you.

The Traffic Tab

The Traffic tab provides information for analyzing traffic on switches and wireless LAN controllers. The four monitors provide an aggregated view of all network traffic on a device, such as proportion of current proportion of multicast, unicast, broadcast traffic or the trend in packet errors. Tasks provide more detailed looks at traffic, such as traffic statistics for individual ports or the degree in which a port's bandwidth is being used.

The Client Tab

The Client tab provides information about clients and sessions on the network. A client is any device that is connected to the network through a wireless access point or through an access port on a switch that is an 802.1X authenticator port. Examples of clients include VoIP phones, laptops, printers, security cameras, and so on. When a client connects to the network, a session starts, which is uniquely identified by the MAC address of the client.

The Client tab monitors provide a view of overall client session activity in the selected scope. They show the total number of sessions, sessions consuming the most bandwidth, and trends in the number of sessions. Detailed views provide information about each client, such as MAC address, IP address, username, client VLAN, and port or wireless access point the client is connected to. You can also search for a particular client session or sessions using a variety of search criteria and view client history.

NOTE: **Because traffic information is unavailable for sessions connected to access ports on switches, monitors that show session traffic, such as the Top Sessions by MAC Address monitor, are not displayed for scopes that contain switches only.**

The RF Tab

The RF tab provides information about the wireless environment and signal performance, allowing you to identify problems that affect wireless connectivity. Monitors provide information about throughput, retransmissions, packet errors, signal-to-noise ratio, and interference sources. Tasks enable you to determine a radio's neighbors and to display spectrograms for troubleshooting interference.

The Equipment Tab

The Equipment tab provides information about the operational status of individual devices. Monitors display CPU and memory use, power supply and fan status, port status, and general device information for switches and wireless LAN controllers. The status of access point and radios is displayed when you select their wireless LAN controller. Additional information provided by this tab includes the state of logical Ethernet switching interfaces on standalone switches, the topology of Virtual Chassis, and the list of access points that use a selected controller as a secondary controller.

The Fabric Analysis Tab

The Fabric Analysis tqb displays the results of running the Run Fabric Analyzer task on a QFabric device. It shows information about the health, connectivity, and topology of the QFabric. For information about analyzing QFabric devices, see "Analyzing QFabric Devices" on page 57.

Related Documentation

- Understanding the Monitor Mode Tasks Pane on page 11
- *Understanding the Network Director User Interface*

Understanding the Monitor Mode Tasks Pane

The Tasks pane in Monitor mode displays a list of tasks that are available for the currently selected Monitor tab. These tasks provide monitoring functions in addition to the monitors available under each tab.

The tasks listed in the Tasks pane vary according to the selected tab—that is, Summary, Traffic, Client, RF, or Equipment—and the scope you have selected in the View pane. For example, the VC Protocols Statistics task is available only when you select the Traffic tab and a Virtual Chassis or Virtual Chassis member in the View pane.

For each Monitor mode tab, the following tables list each task and provide a short description of the task and the scope it is available in:

- Table 3 on page 11: Summary Tab Tasks
- Table 4 on page 12: Traffic Tab Tasks
- Table 5 on page 13: Client Tab Tasks
- Table 6 on page 13: RF Tab Tasks
- Table 7 on page 14: Equipment Tab Tasks
- Key Tasks—Network Director enables you to group the tasks that you perform frequently and create a list of key tasks. You can add any task from the Tasks pane to the Key Tasks list by selecting a task and clicking the plus (+) sign that appears adjacent to the task. For some modes, you can see that Network Director has predefined some key tasks for you. You can modify this set of tasks to suit your requirements. This feature is available in Task pane irrespective of your current mode, scope, or view.
- For information about the Fabric Analysis tab, see "Analyzing QFabric Devices" on page 57.

Table 3: Summary Tab Tasks

Task	Description	Scope
Backed-Up APs	Displays information about the access points for which the selected controller is the secondary controller in a cluster.	Wireless LAN controller
Compare Device Statistics	Compare statistics from multiple devices in real time.	Any
Find End Point	Finds end points that match supplied attributes and returns information about the location of the end points on the network.	My Network, Switches, Unassigned, and EX Series switch
Find User Session	Finds client sessions that match supplied attributes and returns information about the sessions.	My Network
Ping To a Host	From the selected device, pings the host you specify and returns the results.	Standalone switch, Virtual Chassis, QFabric device

Table 3: Summary Tab Tasks *(continued)*

Task	Description	Scope
Port Utilization Trend	Displays a graph showing the trend of bandwidth use for all the ports on all the devices in the selected scope over the last hour.	My Network, mobility domain, standalone switch, Virtual Chassis, or wireless LAN controller, locations
Run Fabric Analyzer	Analyzes a QFabric device and provides information about its health, connectivity, and topology on the Fabric Analysis tab.	QFabric device
Select Monitors to display	Selects the monitors that are displayed in the Summary tab	My Network
Traceroute To a Host	From the selected device, traces the route to the host you specify and returns the results.	Standalone switch, Virtual Chassis, QFabric device

Table 4: Traffic Tab Tasks

Task	Description	Scope
Compare Device Statistics	Compare statistics from multiple devices in real time.	Any
Current Port Utilization	For each port on the selected device, shows the current percentage of port capacity in use.	Any
Find End Point	Finds end points that match supplied attributes and returns information about the location of the end points on the network.	My Network, Switches, Unassigned, and EX Series switch
Find User Session	Finds client sessions that match supplied attributes and returns information about the sessions.	Any
L3 VLAN Statistics	Displays packet in and out statistics for Layer 3 VLANs on the selected device.	Standalone switch and Virtual Chassis only
Ping To a Host	From the selected device, pings the host you specify and returns the results.	Standalone switch, Virtual Chassis, QFabric device
Port Statistics	Displays packet and error statistics for all ports on the selected device.	Standalone switch, Virtual Chassis, or wireless LAN controller
Port Utilization Trend	Displays a graph showing the trend of bandwidth use on the selected device's ports over the last hour.	Any
Run Fabric Analyzer	Analyzes a QFabric device and provides information about its health, connectivity, and topology on the Fabric Analysis tab.	QFabric device
Traceroute To a Host	From the selected device, traces the route to the host you specify and returns the results.	Standalone switch, Virtual Chassis, QFabric device

Table 4: Traffic Tab Tasks *(continued)*

Task	Description	Scope
VC Protocol Statistics	Displays Virtual Chassis Control Protocol (VCCP) statistics for the selected Virtual Chassis or Virtual Chassis member, such as the kind and number of protocol data units (PDUs) sent and received.	Virtual Chassis or Virtual Chassis member only

Table 5: Client Tab Tasks

Task	Description	Scope
Compare Device Statistics	Compare statistics from multiple devices in real time.	Any
Find End Point	Finds end points that match supplied attributes and returns information about the location of the end points on the network.	My Network, Switches, Unassigned, and EX Series switch
Find User Session	Finds client sessions that match supplied attributes and returns information about the sessions.	Any
Ping To a Host	From the selected device, pings the host you specify and returns the results.	Standalone switch, Virtual Chassis, QFabric device
Refresh End Point	Refreshes end point location information for the Find End Point task.	My Network
Run Fabric Analyzer	Analyzes a QFabric device and provides information about its health, connectivity, and topology on the Fabric Analysis tab.	QFabric device
Traceroute To a Host	From the selected device, traces the route to the host you specify and returns the results.	Standalone switch, Virtual Chassis, QFabric device

Table 6: RF Tab Tasks

Task	Description	Scope
Compare Device Statistics	Compare statistics from multiple devices in real time.	Any
Find User Session	Finds client sessions that match supplied attributes and returns information about the sessions.	Any
Interference Sources	Displays the sources of interferences detected by the selected radio.	Radios only
Ping To a Host	From the selected device, pings the host you specify and returns the results.	Standalone switch, Virtual Chassis, QFabric device
Run Fabric Analyzer	Analyzes a QFabric device and provides information about its health, connectivity, and topology on the Fabric Analysis tab.	QFabric device
Spectrogram	Displays a spectrum analysis of the 2.4-GHz and 5-GHz bands.	Radios only

Table 6: RF Tab Tasks *(continued)*

Task	Description	Scope
RF Neighborhood	Displays a list radios that are in the vicinity of the selected radio. These radios are either radios that the selected radio detects or radios that detect the selected radios.	Radios only
Traceroute To a Host	From the selected device, traces the route to the host you specify and returns the results.	Standalone switch, Virtual Chassis, QFabric device

Table 7: Equipment Tab Tasks

Task	Description	Scope
Backed-Up APs	Displays information about the access points for which the selected controller is the secondary controller in a cluster.	Wireless LAN controller
Compare Device Statistics	Compare statistics from multiple devices in real time.	Any
Find End Point	Finds end points that match supplied attributes and returns information about the location of the end points on the network.	My Network, Switches, Unassigned, and EX Series switch
Find User Session	Finds client sessions that match supplied attributes and returns information about the sessions.	Any
Logical Interfaces	Displays the status of the Ethernet switching interfaces on the device, including aggregated Ethernet interfaces. Information includes VLAN membership, STP state, and port mode.	Standalone switch, Virtual Chassis
Ping to a Host	From the selected device, pings the host you specify and returns the results.	Standalone switch, Virtual Chassis, QFabric device
Run Fabric Analyzer	Analyzes a QFabric device and provides information about its health, connectivity, and topology on the Fabric Analysis tab.	QFabric device
Traceroute To a Host	From the selected device, traces the route to the host you specify and returns the results.	Standalone switch, Virtual Chassis, QFabric device

Related Documentation

- Understanding Monitor Mode in Network Director on page 3
- *Understanding the Network Director User Interface*

PART 2

Administration

CHAPTER 2

General

Changing Monitor Polling Interval and Data Collection

Network Administrators can change the default polling interval for monitors. The default polling period varies by monitor category. You can change these values in Preferences, found in the Network Director banner. You can also enable or disable the data collection processes used by monitors in Preferences.

Related Documentation

- *Setting Up User and System Preferences*

Finding End Points

This topic describes how to find end points on the network. End points are computing devices that are connected to the network. You can search for end points based on several attributes. When you find an end point, you can see its last known location in the network.

This topic describes:

Procedure for Finding End Points

1. Click **Monitor** in the Network Director banner.

   You can search for end points in any tab in Monitor mode.

2. In the Tasks pane, select **Tasks** > **Find Endpoint**.

   The Find End Point window opens. For information about this window, click the Help button in the title bar of the window or see "Find End Point Window" on page 18.

Find End Point Window

The Find End Point window enables you to search for end points and see their last known location in the network. The search scope is the entire managed network, regardless of which node is selected in the View pane.

To find end points:

1. Enter search text in the text box. The search looks for the search text in these end point attributes:
   - MAC address
   - IP address
2. Click **Search**.

   The found end points appear in the Search Results table. See Table 8 on page 18 for a description of this table.

Table 8: Table of Found End Points

Table Column	Description
MAC Address	MAC address of the connected end point.
IP Address	IP address of the connected end point.
Device Name	Name of the networking device that last saw the end point on the network.
Interface Name	Name of the device interface that last saw the end point on the network.
VLAN	VLAN on which the end point was last seen.
Last Seen	When the end point was last seen on the network.
Actions	Click **Verify Current Location** to verify the information shown for the end point. If any information changed since the last poll, it is updated in the table.

Refreshing End Point Information

Information about all end points connected to the managed network is polled automatically once every 24 hours. You can refresh this information manually.

NOTE: **Refreshing end point information can consume significant system resources and take several minutes to complete, depending on the size of the network and the number of connected end points.**

To refresh information about all end points connected to the managed network:

1. Click **Monitor** in the Network Director banner.

2. In the Tasks pane, select **Tasks** > **Refresh Endpoint**.

   A confirmation window opens, listing the job ID of the refresh job.

The endpoint refresh runs as a job. You can monitor the job status in System mode by selecting **Tasks** > **Manage Jobs** in the Task pane.

Related Documentation

- Understanding the Monitor Mode Tasks Pane on page 11

Selecting Monitors To Display on the Summary Tab

When you select the My Network node in the View pane, the Summary tab in Monitor mode enables you to select which monitors to display. If you select more than four monitors, a scroll bar appears to allow you to scroll to the additional monitors.

To select monitors to display on the Summary tab:

1. Click **Monitor** in the Network Director banner.
2. Select the **My Network** node in the View pane (the top node in the tree).
3. To select which monitors to display on the Summary tab:
   a. Click **Select Monitors to Display** in the Tasks pane.

      The Select Monitors window opens. The monitors that are already selected to display are listed in the Selected list. The other available monitors are listed in the Available list.

   b. To move a monitor from one list to the other list, click the monitor name, and then click the right or left arrow button, as appropriate.

   c. To change the order in which the selected monitors appear in the tab, select a monitor name and move it in the list using the up and down arrow buttons. The arrow buttons at the top and bottom of the stack of buttons move the selected monitor to the top or bottom of the list, respectively.

   d. Click **Save** to save your changes, or click **Cancel** to cancel your changes.
4. To get information about a monitor, click the Help button in its title bar.

Related Documentation

- Understanding Monitor Mode in Network Director on page 3

Pinging Host Devices

Use the Ping Host task in Monitor mode to determine whether an EX Series host can be reached over the network from the device selected in the network tree. Entering a hostname or an address creates a periodic ping task that sends a series of Internet Control Message Protocol (ICMP) echo (ping) requests to the specified host. The output of the task displays in the Response Console.

The Ping from Device to a Host task is available only for EX Series switches and QFX Series switches in your network.

1. Select either IP or HostName in the Remote Host Details box.
2. Type the IP address or hostname for the device that you want to reach.
3. Click **Ping** to use the default settings and start the requests or select the plus (+) symbol to use the Advanced Search Criteria. The fields in Advanced Search Criteria are described in Table 9 on page 20.

Table 9: Ping Host Advanced Search Criteria Field Descriptions

Field	Description	Default
Count	Indicates the number of ping requests to send. Valid values are 1 through 24.	3
Type of Service	Sets the type-of-service (ToS) field in the IP header of the ping packets. The range of values is 0 through 255. If the routing platform does not support ToS, the field is ignored.	0
Time To Live	Indicates the time-to-live hop count for the ping request packet. Valid values are 0 through 255.	32
Wait Interval	Indicates the amount of time in seconds between ping requests. Valid values are 0 through 24; a 0 value sends the request immediately.	0
Packet Size	Indicates the size of the ping request packet in bytes. The routing platform adds 8 bytes of ICMP header to this size before sending the request packet.	56
Interface	Sends the ping requests on the interface you specify. Iif you do not specify this option, ping requests are sent on all interfaces.	All
Source	Uses the source address that you specify in the ping request packet.	None

Related Documentation

- Understanding Monitor Mode in Network Director on page 3

CHAPTER 3

Monitoring Traffic

Monitoring Traffic on Devices

The monitors on the Traffic tab provide information about the traffic traversing switches, Virtual Chassis, and wireless controllers.

To monitor traffic on a device:

1. Click **Monitor** in the Network Director banner.
2. Select the switch, Virtual Chassis, or wireless controller in the View pane that contains the traffic you want to monitor.
3. Select the **Traffic** tab to open the traffic monitors.
4. To get help for a monitor, click the Help button in its title bar.

The available monitors are:

- "Unicast vs Broadcast/Multicast Monitor" on page 113: shows the distribution of unicast, broadcast, and multicast traffic entering and leaving the device.
- "Unicast vs Broadcast/Multicast Trend Monitor" on page 113: shows trend data about the distribution of unicast, broadcast, and multicast traffic entering and leaving the device.
- "Traffic Trend Monitor" on page 112: shows trend data about the amount of traffic entering and leaving the device.
- "Error Trend Monitor" on page 81: shows trend data about the amount of errors on the device.

Related Documentation

- Understanding Monitor Mode in Network Director on page 3
- Monitoring Port Traffic Statistics on page 22

Monitoring Port Traffic Statistics

This topic describes how to monitor port traffic statistics on a device. You can monitor port traffic statistics for a switch, Virtual Chassis, or wireless controller node in any view.

This topic describes:

Procedure for Monitoring Port Traffic Statistics

1. Click **Monitor** in the Network Director banner.
2. Select a node in the View pane that contains the port traffic you want to monitor.
3. Select the **Traffic** tab.
4. In the Tasks pane, select **View** > **Port Statistics**.

   The Port Traffic Stats window opens. For information about this window, click the Help button in the title bar of the window or see "Port Traffic Stats Window" on page 22.

Port Traffic Stats Window

The Port Traffic Stats window displays information about the port traffic on the node you selected in the View pane. It contains the following elements:

- Port Traffic Trend graph—This line graph shows trends in the data and error rates on the port selected in the ports table below it. The horizontal axis shows the times when samples were taken. The vertical axis shows the data rate on the left side (in bytes per second) and the error rate on the right side (in errors per second).

  To display traffic for a different port, select the port from the table below the graph. To change the time period over which to display the traffic trends, select a time period from the list in the upper right corner.

  NOTE: **After a device is discovered, trend data does not appear immediately—it appears only after three polling periods have elapsed.**

  To highlight a line on the graph, mouse over the line legend. To remove or restore a line, click the line legend. To see numeric values, mouse over where a data line intersects with a dotted vertical grid line.

- Ports table (on the lower left side of the window)—This table provides information about the ports as described in Table 10 on page 23. Selecting a port from this table

updates the Port Traffic Trend graph to display traffic information about the selected port.

- Counter selection table (on the lower right side of the window)—This table enables you to select which counters to display on the Port Traffic Trend graph. It includes separate tabs for packet counters and error counters. Select the check box in the Show column of each counter that you want to display on the graph. The Per/Sec column shows the rate per second of that row's counter.

Table 10: Port Traffic Window

Table Column	Description
Port Name	Port name.
MAC Addresses	Port MAC address.
Link Type	Port link type.
In Packets/Sec.(Current)	Current rate of inbound packets.
Out Packets/Sec.(Current)	Current rate of outbound packets.

Related Documentation

- Understanding the Monitor Mode Tasks Pane on page 11

Monitoring Port Traffic Utilization Trends

This topic describes how to monitor port traffic utilization trends. You can monitor port traffic utilization for a switch, Virtual Chassis, wireless controller, wireless cluster, and wireless network, in any view.

This topic describes:

- Procedure for Monitoring Port Traffic Utilization on page 23
- Port Traffic Utilization Count Window on page 24

Procedure for Monitoring Port Traffic Utilization

1. Click **Monitor** in the Network Director banner.
2. Select a node in the View pane that contains the port traffic you want to monitor.
3. Depending on the node type you selected in the View pane, this task might be available on the Summary or Traffic tab, or both tabs.
4. In the Tasks pane, select **View** > **Port Utilization Trend**.

   The Port Traffic Utilization Count window opens. For information about this window, click the Help button in the title bar of the window or see "Port Traffic Utilization Count Window" on page 24.

Port Traffic Utilization Count Window

The Port Traffic Utilization Count window displays a bar chart with information about the port traffic utilization on the node selected in the View pane. Each bar in the chart represents the port traffic utilization data gathered at a polling interval. The vertical axis shows the number of ports polled. The horizontal axis shows the time when each poll was taken. The data shown in the graph is aggregated from all the ports contained in the node selected in the View pane.

Each bar is divided into the following colored sections to indicate the distribution of port traffic utilization at the polling interval:

- Green indicates ports that operated at less than 50% of negotiated speed.
- Orange indicates ports that operated at between 50% and 80% of negotiated speed.
- Red indicates ports that operated at more than 80% of negotiated speed.

You can perform the following actions on the bar chart:

- Change the time period over which to display the data by selecting a time period from the list in the upper right corner.
- Remove or restore a utilization category (bar color) by clicking its legend.
- Display a numeric value by mousing over a bar.

Related Documentation

- Understanding the Monitor Mode Tasks Pane on page 11

Monitoring Virtual Chassis Protocol Statistics

This topic describes how to monitor Virtual Chassis protocol statistics on a device. You can monitor Virtual Chassis protocol statistics for a Virtual Chassis node in any view.

This topic describes:

Procedure for Monitoring Virtual Chassis Protocol Statistics

1. Click **Monitor** in the Network Director banner.
2. Select a node in the View pane that contains the Virtual Chassis protocol traffic you want to monitor.
3. Select the **Traffic** tab.
4. In the Tasks pane, select **View** > **VC Protocol Statistics**.

   The Virtual Chassis Protocol Statistics window opens. For information about this window, click the Help button in the title bar of the window or see "Virtual Chassis Protocol Statistics Window" on page 25.

Virtual Chassis Protocol Statistics Window

The Virtual Chassis Protocol Statistics window displays information about the Virtual Chassis protocol statistics on the Virtual Chassis node you selected in the View pane. It contains these panes:

- The top pane of the window lists the Virtual Chassis members and provides the information about each member that is described in Table 11 on page 25.

  Select a member's table row to see information about that member in the other panes.

- The middle and bottom panes provide the information described in Table 12 on page 25.

Table 11: Virtual Chassis Protocol Statistics Window Top Pane

Table Column	Description
Member	Virtual Chassis member's ID.
Role	Member's Virtual Chassis role. Roles include Master, Backup, and LinecCard.
FPC Slot	Member's FPC slot in the Virtual Chassis.
Member Serial Number	Member's serial number.

Table 12: Virtual Chassis Protocol Statistics Window Middle and Bottom Panes

Field or Table Column	Description
System Name	Member system name.
Purges initiated	Number of purges that the system initiated. A purge is initiated if the software determines that a link-state PDU must be removed from the network.
Shortest-path-first runs	Number of shortest-path-first (SPF) calculations that have been performed.
Link-state PDUs queue length	Number of link-state PDUs waiting in the queue for processing. This value is almost always 0.
Link-state PDU fragments computed	Number of link-state PDU fragments that the local system has computed.
Link-state PDUs regenerated	Number of link-state PDUs that have been regenerated. A link-state PDU is regenerated when it is nearing the end of its lifetime and it has not changed.
Protocol data unit type (PDU)	Protocol data unit type.
PDUs Received	Number of PDUs received since VCCP started or since the statistics were set to zero.
PDUs Processed	Number of PDUs received minus the number of PDUs dropped.
PDUs Dropped	Number of PDUs dropped.

Table 12: Virtual Chassis Protocol Statistics Window Middle and Bottom Panes *(continued)*

Field or Table Column	Description
PDUs Transmitted	Number of PDUs transmitted after VCCP started or after the statistics were set to zero.
PDUs Retransmitted	Number of PDUs retransmitted after VCCP started or after the statistics were set to zero.

Related Documentation

- Understanding the Monitor Mode Tasks Pane on page 11

Monitoring Traffic on Layer 3 VLANs

This topic describes how to monitor Layer 3 VLAN traffic statistics on a device. You can monitor Layer 3 VLAN statistics for a switch or Virtual Chassis node in any view.

This topic describes:

- Procedure for Monitoring Layer 3 VLAN Traffic Statistics on page 26
- L3 VLAN Traffic Stats Window on page 26

Procedure for Monitoring Layer 3 VLAN Traffic Statistics

1. Click **Monitor** in the Network Director banner.
2. Select a node in the View pane that contains the Layer 3 VLAN traffic you want to monitor.
3. Select the **Traffic** tab.
4. In the Tasks pane, select **View** > **L3 VLAN Statistics**.

   The L3 VLAN Traffic Stats window opens. For information about this window, click the Help button in the title bar of the window or see "L3 VLAN Traffic Stats Window" on page 26.

L3 VLAN Traffic Stats Window

The L3 VLAN Traffic Stats window displays information about the Layer 3 VLAN traffic on the node you selected in the View pane. It contains two panes:

- VLAN Traffic line graph—This graph shows the data transmission rate on the Layer 3 VLAN selected in the table below. The horizontal axis shows the times when samples were taken. The vertical axis shows the data rate, in bytes per second.

  To show a Layer 3 VLAN on the VLAN Traffic line graph, select the Layer 3 VLAN from the table below. To highlight a line on the graph, mouse over the line legend. To remove or restore a line, click the line legend. To see numeric values, mouse over where a data line intersects with a dotted vertical grid line.

- Layer 3 VLAN traffic statistics table—This table provides information about the Layer 3 VLANs as described in Table 13 on page 27. Selecting a Layer 3 VLAN from this table

updates the VLAN Traffic graph to display the traffic information for the selected Layer 3 VLAN.

Table 13: Layer 3 VLAN Traffic Statistics Table

Table Column	Description
L3 Interface	Layer 3 interface assigned to the VLAN.
VLAN Name	VLAN name.
VLAN ID	VLAN ID.
Description	VLAN description.
In Packet	Number of packets entering the VLAN.
Out Packet	Number of packets leaving the VLAN.

Related Documentation

- Understanding the Monitor Mode Tasks Pane on page 11

CHAPTER 4

Monitoring Client Sessions

Monitoring Client Sessions

The Client tab in Monitoring mode provides information about clients and sessions on the network. It is available when the node you select in the View pane contains client and session data. The types of available monitoring data vary depending on the node or node type selected.

To monitor client sessions:

1. Click **Monitor** in the Network Director banner.
2. Select a node in the View pane that contains the client sessions you want to monitor.
3. Select the **Client** tab.
4. To get information about a monitor, click the Help button in its title bar.

The Client monitors include:

- "Top Users Monitor" on page 111: shows the clients that use the most bandwidth.
- "Top Sessions by MAC Address Monitor" on page 109: shows the sessions that use the most bandwidth.
- "Session Trends Monitor" on page 99: shows trends about the number of active sessions.
- "Current Sessions Monitor" on page 79: shows the current active sessions.

Related Documentation

- Understanding Monitor Mode in Network Director on page 3
- Finding User Sessions on page 30

Finding User Sessions

This topic describes how to find user sessions on the network. You can search for sessions based on several session attributes. When you find a session, you can view its current and historical bandwidth usage.

This topic describes:

Procedure for Finding User Sessions

1. Click **Monitor** in the Network Director banner.

   You can search for user sessions in any tab in Monitor mode.

2. In the Tasks pane, select **Tasks** > **Find User Session**.

   The Search User Session window opens. For information about this window, click the Help button in the title bar of the window or see "Search User Session Window" on page 30.

Search User Session Window

The Search User Session window enables you to search for and view information about user sessions. The search scope is the entire managed network, regardless of which node is selected in the View pane. You can view current and historical session information.

To find user sessions:

1. Enter search text in the text box. The search looks for the search text in these session attributes:
   - MAC address
   - IP address (IPv4 or IPv6)
   - User name
2. Click **Search**.

   The found user sessions appear in a table. See Table 14 on page 31 for a description of this table.

3. To view more information about a session, click its table row.

   Detailed information about the session appears. The MAC address appears at the top of the page. The page contains these sections:

   - Current Session Information—Displays information about the current session. Table 15 on page 31 describes the information shown for sessions connected to the network by a wireless connection. Table 16 on page 32 describes the information shown for sessions connected to the network by a wired connection.

- Past Session Information—Displays information about the MAC addresses'' past sessions. This information is not shown for sessions connected to the network by a wired connection. You can select the time period to view from the list above the table. Table 17 on page 32 describes the information shown.

4. When you are done viewing a session's details, to return to the search results, the **Back** button in the top left corner of the window.

Table 14: User Session Details Table for Found User Sessions

Table Column	Description
MAC Address	MAC address of the connected device.
Client IPv4	IP version 4 address of the connected device.
User Name	User name of the connected user.
Session Type	Shows whether the session is connected by wired or wireless connection.
Client IPv6	IP version 6 address of the connected device.
Link-local	Link-local address.

Table 15: Current Session Information for Found Wireless User Sessions

Field	Description
User Name	User name of the connected user.
Session Started On	Time when the current session started.
Elapsed Time	Length of time the session has been active.
Client IP	IP address of the connected device. Includes IPv4 and IPv6 addresses.
Controller IP	IP address of the controller to which the client is connected.
VLAN	Name of the VLAN the session is using.
SSID	SSID of the wireless LAN to which the session is connected.
RSSI	Received signal strength indication (RSSI), in decibels referred to 1 milliwatt (dBm). A higher value indicates a stronger signal.
SNR Value	Signal-to-noise ratio (SNR), a measure of the level of a desired signal against the level of background noise, measured in decibels (dB).
Session Location	The physical location of the wireless access point serving the session. The physical location has the hierarchy site-building-floor.

Table 15: Current Session Information for Found Wireless User Sessions *(continued)*

Field	Description
Client Device Type	Client's device type.
Client Device Group	Client's device group.
Client Device Profile	Client's device profile.
Receive Unicast KBytes	Unicast bytes received by the session.
Transmit Unicast KBytes	Unicast bytes transmitted by the session.
Receive Multicast KBytes	Multicast bytes received by the session.
Data Usage (KBytes)	Data transmitted and received by the client, in kilobytes.
Roaming History	Shows the session's roaming history in a table with these columns: • Start Time—Time when the session connected to the wireless access point. • AP Name—Name of the wireless access point to which the session connected.

Table 16: Current Session Information for Found Wired User Sessions

Field	Description
Username	Username of the connected user.
Device IP	IP address of the device.
Authentication Type	Type of authentication used to authenticate the session.
VLAN	Name of the VLAN the session is using.
Device Serial	Device's serial number.
Port	Port to which the device is connected.

Table 17: Past Session Information for Found User Sessions

Table Column	Description
Session Start Time	Time when the current session started.
Elapsed Time	Length of time the session has been active.
Client IPv4	IP version 4 address of the connected device.
Client IPv6	IP version 6address of the connected device.

Table 17: Past Session Information for Found User Sessions *(continued)*

Table Column	Description
Link-local	Link-local address.
Controller IP	IP address of the controller to which the client is connected.
SSID	SSID of the wireless LAN to which the session is connected.
VLAN	VLAN to which the client is connected.
RSSI	Received signal strength indication (RSSI), in decibels referred to 1 milliwatt (dBm). A higher value indicates a stronger signal.
SNR	Signal-to-noise ratio (SNR), a measure of the level of a desired signal against the level of background noise, measured in decibels (dB).
RxUnitBytes Value	Unicast bytes received by the session.
RxMultiBytes Value	Unicast bytes transmitted by the session.
TxUnitBytes Value	Multicast bytes received by the session.
Data Usage (KBytes)	Data transmitted and received by the client, in kilobytes.

Related Documentation

- Understanding the Monitor Mode Tasks Pane on page 11

CHAPTER 5

Monitoring Radio Frequency (RF)

Monitoring RF 802.11 Packet Errors

Damaged packets cannot be read by devices, therefore they are discarded and re-sent if they are data packets. (See "Monitoring the Percentage of RF Packet Retransmissions" on page 48.) This increases the number of re-sent packets and decreases the throughput on the network. (See "Monitoring RF Throughput" on page 47.) Voice and video packets are dropped but not re-sent, decreasing the quality of VoIP and streamed media. Packet errors can occur when:

- Noise causes spurious packets.
- Signal degradation occurs causing a weak signal.
- Channels are too congested, causing packet collision and corruption.
- Hardware or drivers are faulty.
- Excessive packets are being received from one source—this could be a flood attack.

In Network Director, at the configured interval (set in *Setting Up User and System Preferences*), the total number of 802.11 packet errors is compiled and plotted on a line chart monitor. You can monitor packet errors for the following:

- An access point
- A radio
- An entire site
- A building
- A floor of a building
- A wiring closet

NOTE: **Unlike access points and radios, which appear on the list automatically, sites, buildings, floors and wiring closets must be configured by you.**

To view RF packet errors over a fixed period of time:

1. Select **Monitor** Mode in the Network Director banner.
2. Select any view from the View pane.
3. Expand the list in the View pane, then select one of the objects listed in Table 18 on page 36:

Table 18: Objects in the View Pane

Icon	Object
	Individual radio

Table 18: Objects in the View Pane *(continued)*

Icon	Object
	Individual access point
	Wiring closet—to create a wiring closet, see *Setting Up Closets*.
	Selecting a floor in logical view displays all access points on that floor—to create a floor, see *Configuring Floors*.
	Selecting a building in logical view displays all access points in that building—to create a building, see *Configuring Buildings*.
	Selecting a site from the logical view displays all access points in that building—to create a site, see *Creating a Site*.

The Monitor mode RF tab becomes available when you select one of the objects listed in Table 18 on page 36 .

4. Click the Monitor mode **RF** tab to view the four basic monitors, which includes the RF packet error monitor.

   The populated RF Packet Errors monitor opens, displaying the number of packet errors that the selected object has experienced over the past hour.

5. Optionally, change the timeframe covered by the monitor by selecting a different time from the list.

6. Click **Help** (?) for help interpreting the throughput chart or see "802.11 Packet Errors Monitor" on page 76.

Related Documentation

- 802.11 Packet Errors Monitor on page 76
- Monitoring the Percentage of RF Packet Retransmissions on page 48
- *Configuring Floors*
- *Configuring Buildings*
- *Creating a Site*
- Monitoring RF Throughput on page 47

Monitoring RF Interference Sources For Radios on One Access Point

Because the 2.4-GHz band includes radio transmissions from devices other than wireless networks, interference is a common problem. Network Director detects, classifies, and displays radio interference in several monitors. This topic describes the access point interference monitor that can be applied only to access points. If the access point has two radios, interference for each is displayed separately.

NOTE: You can also monitor interference by "Monitoring RF Interference Sources on One Radio" on page 38 and "Monitoring RF Interference Sources on Wireless Devices" on page 41.

To view an access point's RF interference sources over a fixed period of time:

1. Select **Monitor** Mode in the Network Director banner.
2. Select any view from the View pane.
3. Expand the wireless list in the View pane, then select an access point.

   The RF monitor tab becomes available when you select an access point.
4. Click the **RF** tab.

   The RF Interference Sources monitor bar chart for access point radios is displayed as one of the four default monitors.
5. Optionally, change the timeframe covered by the monitor by selecting a different time from the list.
6. Optionally, add or remove a radio on the chart by clicking **Radio1** or **Radio2** in the legend.
7. Click **Help** (?) for information about the access point interference chart or see "RF Interference Sources Monitor For an Access Point" on page 93.

Related Documentation

- RF Interference Sources Monitor For an Access Point on page 93
- Monitoring RF Interference Sources on One Radio on page 38
- Monitoring RF Interference Sources on Wireless Devices on page 41
- Understanding Wireless Interference on page 54

Monitoring RF Interference Sources on One Radio

Because the 2.4-GHz band includes radio transmissions from devices other than wireless networks, interference is a common problem. Network Director detects, classifies, and displays radio interference in several monitors. This topic describes monitoring the interference of one radio displayed in a pie chart.

NOTE: You can also monitor interference by "Monitoring RF Interference Sources on Wireless Devices" on page 41 and "Monitoring RF Interference Sources For Radios on One Access Point" on page 38.

Monitoring RF Radio Interference Sources

To view a radio's RF interference sources in a pie chart over a fixed period of time:

1. Select **Monitor** Mode in the Network Director banner.
2. Select any view from the View pane.
3. Expand the wireless list in the View pane, then select a radio.

   The monitor mode RF tab becomes available when you select a radio.
4. In the Tasks pane on the right, click **Interference Sources**.

   A pie chart is displayed with a breakdown of the interference sources detected on the selected radio.
5. Optionally, change the timeframe covered by the monitor by selecting a different time from the list.
6. Click **Help** (?) for information about the radio interference chart or see "RF Interference Sources Pie Chart for a Radio" on page 39.

NOTE: To change the polling interval for monitors, see *Setting Up User and System Preferences*.

RF Interference Sources Pie Chart for a Radio

The RF Interference Sources pie chart for a single radio reflects all devices that have interfered with the traffic of the radio selected in the View pane. Network Director tracks and monitors interference from these sources:

- Microwave ovens—Most domestic microwave ovens use 2.45 GHz, and can interfere with Wi-Fi channels from 8 to 10 (or even 7 to 11). Interference varies depending on the model of the oven—for example, commercial restaurant microwave ovens sweep over a wider spectrum and have a higher duty cycle.
- Continuous wave devices continuously transmit at a particular frequency without attempting to share the radio frequency medium with other devices. Devices that use continuous wave technology in the same frequency bands as wireless LAN networks will interfere with wireless communications, reducing performance or totally preventing communication. Several examples of devices that use continuous wave transmission that interferes with WiFi are video surveillance cameras and baby monitors.

- Bluetooth devices
- Phone FHSS from cordless phones
- Unknown devices

To track these interference devices, Network Director polls the access point's controller at the standard interval. The categories with the largest sections of the pie cause the most radio interference.

You can perform the following actions on the pie chart:

- Change the time period over which to display interference by selecting a time period from the list in the upper right corner.
- Display a numeric value for interference objects by mousing over a section of the chart.
- Click the monitor's title to see a list of interference incidents along with the information listed in Table 19 on page 40.

Table 19: Information on RF Interference Sources for a Radio

Information	Description
Last Seen	Date and time the interference was last detected.
Transmitter ID	If the interference is caused by an object with a MAC address, the MAC address is displayed. If the object has no MAC address, MSS calculates a MAC address, using the characteristics of the object. This way, you can correlate interference events over time.
Listener MAC	MAC address of the access point that detected the interference.
AP	Name of the access point that detected the interference.
Controller	Name of the controller that reported the interference.
Channel	Channel the interference affected.
RSSI	Received signal strength indication (RSSI), in decibels referred to 1 milliwatt (dBm). A higher value indicates a stronger signal.
Duty Cycle	Reported fraction of time that the source is emitting RF.
Source Type	Possible sources of interference include Bluetooth, Continuous Wave, Microwave Oven, Unknown, and Phone FHSS.
CIM (%)	Estimated severity of interference on this channel caused by the source.

Interference is frequently not a problem on wireless networks with light traffic, but as traffic becomes heavier, throughput and capacity decrease and other problems become apparent. RF interference can cause packet retransmission (see "Monitoring the Percentage of RF Packet Retransmissions" on page 48). Interference is also a security concern because jamming can bring down the network .

Ideally, interference retransmission does not cause more than 10% of the total number of packets sent. If your retransmission percentage is higher, you can try to lower it by:

- Locating and eliminating offending devices. If the item cannot be removed, you can add electromagnetic interference (EMI) shielding such as grounded mesh, foils, insulating foams, or insulating paint. This will limit the interference to a small area.
- Moving the affected access point.
- Moving clients to channels with less interference. Keep in mind, however, that Bluetooth devices, cordless phones, 802.11FH devices, and jamming emissions are broadband, so it's not possible to change channels away from them—they are everywhere in the band. For more information, see *Understanding Wireless Radio Channels* and *Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks*.

For more information about wireless interference, see "Understanding Wireless Interference" on page 54.

Related Documentation

- Understanding Wireless Interference on page 54
- Monitoring the Percentage of RF Packet Retransmissions on page 48
- Monitoring RF Interference Sources on Wireless Devices on page 41
- Monitoring RF Interference Sources For Radios on One Access Point on page 38

Monitoring RF Interference Sources on Wireless Devices

Because the 2.4-GHz band includes radio transmissions from devices other than wireless networks, interference is a common problem. Network Director detects, classifies, and displays radio interference in several monitors. This topic describes the Summary interference monitor that can be applied to various wireless objects such as a radio, an access point, a controller cluster, or an entire wireless network.

NOTE: You can also monitor interference by "Monitoring RF Interference Sources on One Radio" on page 38 and "Monitoring RF Interference Sources For Radios on One Access Point" on page 38.

To view a wireless object's RF interference sources over a fixed period of time:

1. Select **Monitor** Mode in the Network Director banner.
2. Select any view from the View pane.
3. Expand the wireless list in the View pane, then select one of the objects listed in Table 20 on page 42.

Table 20: Wireless Objects in the View Pane

Icon	Object
	Entire Wireless Network in any view.
	Wireless Mobility Domain in any view.
	Controller Cluster in any view. NOTE: You cannot see interference for a single controller.
	Individual access point in any view.
	Individual radio in any view.
	Selecting a floor in logical view displays all access points on that floor—to create a floor, see *Configuring Floors*.
	Selecting a building in logical view displays all access points in that building—to create a building, see *Configuring Buildings*.
	Selecting a site from the logical view displays all access points in that building—to create a site, see *Creating a Site*.
	Wiring closet—to create a wiring closet, see *Setting Up Closets*.

The Summary monitor tab becomes available when you select one of the objects listed in Table 20 on page 42.

4. Click the **Summary** tab.

   The RF Interference Sources Summary monitor is displayed as one of the four default monitors.

5. Optionally, change the timeframe covered by the monitor by selecting a different time from the list.

6. Optionally, click the monitor's title to see a list of interfering objects along with the information listed in Table 21 on page 42.

Table 21: Information on RF Interference Sources for a Radio

Information	Description
Last Seen	Date and time the interference was last detected.
Transmitter ID	If the interference is caused by an object with a MAC address, the MAC address is displayed. If the object has no MAC address, MSS calculates a MAC address, using the characteristics of the object. This way, you can correlate interference events over time.
Listener MAC	MAC address of the access point that detected the interference.

Table 21: Information on RF Interference Sources for a Radio *(continued)*

Information	Description
AP	Name of the access point that detected the interference.
Controller	Name of the controller that reported the interference.
Channel	Channel the interference affected.
RSSI	Received signal strength indication (RSSI), in decibels referred to 1 milliwatt (dBm). A higher value indicates a stronger signal.
Duty Cycle	Reported fraction of time that the source is emitting RF.
Source Type	Possible sources of interference include Bluetooth, Continuous Wave, Microwave Oven, Unknown, and Phone FHSS.
CIM (%)	Estimated severity of interference on this channel caused by the source.

7. Click **Help** (?) for information on the RF Interference Sources chart or see "RF Interference Sources Monitor for Wireless Devices" on page 95.

NOTE: To change the polling interval for monitors, see *Setting Up User and System Preferences*.

Related Documentation

- RF Interference Sources Monitor for Wireless Devices on page 95
- Monitoring RF Interference Sources on One Radio on page 38
- Monitoring RF Interference Sources For Radios on One Access Point on page 38
- Understanding Wireless Interference on page 54

Monitoring the RF Neighborhood

View a radio's neighbors with this list. There are two options for viewing the neighboring devices of a radio. You can either view the results of a selected radio's scan for neighbors, or you can view the result when all other radios in the network found the selected radio. This topic describes both options.

This topic describes:

- Procedure for Viewing a Radio's Neighbors on page 43
- RF Neighborhood List on page 44

Procedure for Viewing a Radio's Neighbors

You can monitor the access points operating in the neighborhood of a specified radio.

To view a radio's neighbors:

1. Select **Monitor** Mode in the Network Director banner.
2. Select any View from the View pane.
3. Expand the list in the View pane, and then select a radio.

   The RF monitor tab becomes available when an access point or a radio is selected. The neighbors data is available only for radios.
4. Click the Monitor mode **RF** tab. The four basic radio monitors are displayed.
5. Click **Show Neighbors** in the Tasks pane on the right.

   The current neighbors for the selected radio are displayed with a list of transmitters heard by this radio.
6. Select either of the options: **Transmitters heard by this radio** or **Listeners that heard this radio**. Table 22 on page 44 describes these options.

Table 22: Neighbor Tracking Options

Field	Action
Transmitters heard by this radio (default)	Select to view the selected radio's scan results for other transmitters in the neighborhood of the radio.
Listeners that heard this radio	Select to view a list of other radios on the network that can hear the selected radio.

7. Click **Help** (?) for information about the RF Neighborhood list or refer to the "RF Neighborhood List" on page 44.

RF Neighborhood List

The RF Neighborhood list includes either the neighbors located by the radio you indicated in the View pane or the neighbors that can hear the radio you indicated in the View pane. Determine which way the data will be displayed by selecting either **Transmitters heard by this radio** or **Listeners who heard this radio**. Either way, the neighbor details reported are described in Table 23 on page 44.

Table 23: Data For Neighbors Located by the Radio Scan

Field	Description
Neighbor	Wireless access point radio in close enough proximity to be detected by another access point radio.
BSSID	Identifier for an access point.

Table 23: Data For Neighbors Located by the Radio Scan *(continued)*

Field	Description
Channel	Number of the channel used by the neighbor radio—in the 2.4-GHz band, this is usually 1,6, an 11 in the US. In the rest of the world, channels 1, 5, 9, and 13 are used most often. The 5-GHz band has 24 usable channels, (36,1) (40,-1) (44,1) (48,-1) (52, 1) (56,-1) (60,1) (64,-1) (100,1) (104,-1) (108,1) (112,-1) (116,1) (120,-1) (124,1) (128,-1) (132,1) (136,1) (149,1) (153,-1) (157,1) (161,-1). The +1 and -1 indicated for some channels above indicate channel bonding, where a channel bonds with the one above or below it.
RSSI	Received signal strength indicator (RSSI) is the relative received strength of a signal in a wireless environment. RSSI is basically an indication of the power level being received by the antenna—therefore, the higher the RSSI number, the stronger the signal. (Because the numbers are negative, -50 represents a stronger signal than -88.)

You can perform the following actions on this list:

- Re-sort the list based on the values in any column by mousing over the column title, and then selecting one of these options from the list that appears:
  - Sort Ascending
  - Sort Descending

NOTE: The RSSI column also has a built-in arrow in the title that sorts the list by RSSI order.

- Remove any of the displayed columns by mousing over the column title, selecting **Columns** from the list that appears, and then adding or removing the check marks from Neighbor, BSSID, Channel, or RSSI.

RF neighbor information is available only for radios.

NOTE: To change the polling interval for monitors, see *Setting Up User and System Preferences*.

Related Documentation

- *Understanding Wireless Scanning*

Monitoring RF Signal-to-Noise Ratio

Signal-to-noise ratio (SNR) is a measure of the level of a desired signal against the level of background noise, measured in decibels (dB). Think of having a conversation in an empty restaurant where your signal (your voice) is clearly heard. Now, think of that same restaurant at noon, when the background noise (all other conversations) is at a peak. You will need to talk louder and lean closer to be heard at noon. In other words, you must increase your signal to overcome the background noise.

Signal-to-noise ratio, along with the bandwidth and channel capacity of a communication channel, affects throughput (see "Monitoring RF Throughput" on page 47), especially video throughput.

To view the signal-to-noise ratio on a radio over a fixed period of time:

1. Select **Monitor** Mode in the Network Director banner.
2. Select any view from the View pane.
3. Expand the wireless list in the View pane, then select a radio.

   The Monitor mode RF tab becomes available when you select a radio. The Signal-to-Noise Ratio monitor becomes available only when you select a radio.
4. Click the Monitor mode **RF** tab to view the four basic monitors for radios, which includes the Signal-to-Noise Ratio monitor.

   By default, the populated Signal-to-Noise Ratio monitor graph uses throughput that the selected object has experienced over the last hour.
5. Optionally, change the timeframe covered by the monitor by selecting a different time from the list.
6. Click **Help** (?) for help interpreting the throughput chart or see "Signal-to-Noise Ratio Monitor" on page 101.

NOTE: To change the polling interval for monitors, see *Setting Up User and System Preferences*.

If you are using MSS version 8.0 or higher, you can try using Transmit beam-forming (TxBF) to improve your SNR values. TxBF is a technique that uses an array of transmitting antennas to send radio signals with adjusted magnitude and phase at each antenna to achieve a focused beam target to the receiver. TxBF can increase the Signal-to-Noise Ratio (SNR) at the receiver and improve performance. This feature is supported on the WLA532, WLA321, and WLA322, and is configured from the MSS CLI.

Related Documentation

- Signal-to-Noise Ratio Monitor on page 101
- Monitoring RF Throughput on page 47
- Monitoring the Percentage of RF Packet Retransmissions on page 48

Monitoring RF Throughput

Network throughput is the average rate of successful message delivery over a communication channel. The larger the channel capacity or bandwidth, the greater the potential throughput. There are also factors that reduce WLAN throughput, such as:

- Network load and congestion
- Encryption
- Transmission error correction and packet retransmission of a given packet
- Quality of Service priority settings
- Configuration of the WLAN Service profiles and Radio profiles in use
- Building construction, internal walls and floors, metallic objects
- Mobile clients
- Overhead in the WLAN itself (Layer 2 and below) and overhead in network protocols
- Interference from nearby transmitters using the same frequency

Network Director tracks and monitors the throughput of wireless data for the following wireless objects:

- An access point
- A radio
- An entire site
- A building
- A floor of a building
- A wiring closet

NOTE: **Unlike access points and radios, which appear on the list automatically, sites, buildings, floors and wiring closets must be configured by you.**

To view throughput over a fixed period of time for a selected object:

1. Select **Monitor** Mode in the Network Director banner.
2. Select any view from the View pane.
3. Expand the list in the View pane, and then select one of the objects listed in Table 24 on page 48:

Table 24: Objects in the View Pane With Throughput Data

Icon	Object
	Individual radio
	Individual access point
	Site—Selecting a site in logical view displays all access points on that site—to create a site, see *Creating a Site*.
	Building—Selecting a building in logical view displays all access points in that floor—to create a building, see *Configuring Buildings*.
	Floor—Selecting a floor in logical view displays all access points on that floor—to create a floor, see *Configuring Floors*.

The Monitor mode RF tab becomes available when you select any of the objects listed in Table 24 on page 48 .

4. Click the Monitor mode **RF** tab to view the four basic monitors, which includes the Throughput monitor.

   The populated Throughput monitor opens, displaying the throughput that the selected object has experienced over the last hour.

5. Optionally, change the timeframe covered by the monitor by selecting a different time from the list.

6. Click **Help** (?) for help interpreting the throughput chart or refer to "RF Throughput Monitor" on page 97.

NOTE: To change the polling interval for monitors, see *Setting Up User and System Preferences*.

Related Documentation

- RF Throughput Monitor on page 97
- Monitoring the Percentage of RF Packet Retransmissions on page 48
- *Configuring Floors*
- *Configuring Buildings*
- *Creating a Site*

Monitoring the Percentage of RF Packet Retransmissions

This monitor reflects the percentage of data packets (but not voice packets) that are retransmitted when they do not reach their destination. The higher the percentage of retransmitted data packets, the slower the throughput. (See "Monitoring RF Throughput" on page 47.) Data packets can be retransmitted when:

- Noise causes spurious packets
- Signal degradation occurs causing a weak signal
- Channels are too congested, causing packet collision and corruption
- Hardware or drivers are faulty

Network Director tracks and monitors packet retransmissions for the devices listed in Table 25 on page 49.

This topic describes:

Procedure for Viewing RF Packet Transmission

You can monitor packet transmission for the following:

- An AP
- A radio
- An entire site
- A building
- A floor of a building
- A wiring closet

NOTE: **Unlike access points and radios, which appear on the list automatically, sites, buildings, floors and wiring closets must be configured by you.**

To view RF packet retransmission over a fixed period of time:

1. Select **Monitor** Mode in the Network Director banner.
2. Select any view from the View pane.
3. Expand the list in the View pane, and then select one of the objects listed in Table 25 on page 49:

Table 25: Objects in the View Pane With Packet Retransmission Statistics

Icon	Object
	Individual radio.
	Individual access point.
	Wiring closet—to create a wiring closet, see *Setting Up Closets*.

Table 25: Objects in the View Pane With Packet Retransmission Statistics *(continued)*

Icon	Object
	Selecting a floor in logical view displays all access points on that floor—to create a floor, see *Configuring Floors*.
	Selecting a building in logical view displays all access points in that building—to create a building, see *Configuring Buildings*.
	Selecting a site from the logical view displays all access points in that building—to create a site, see *Creating a Site*.

The Monitor mode RF tab becomes available when you select any of the objects in Table 25 on page 49.

4. Click the Monitor mode **RF** tab to view the four basic monitors, which includes the RF packet retransmission monitor.

   The populated RF packet retransmission monitor opens, displaying the number of packet retransmissions that the selected object has experienced in the last hour.

5. Optionally, change the timeframe covered by the monitor by selecting a different time from the list.

6. Click **Help** (?) for help interpreting the throughput chart or see "Percentage of Packets Retransmitted Monitor" on page 85.

NOTE: To change the polling interval for monitors, see *Setting Up User and System Preferences*.

Related Documentation

- Percentage of Packets Retransmitted Monitor on page 85
- Monitoring RF Throughput on page 47
- *Configuring Floors*
- *Configuring Buildings*
- *Creating a Site*

Monitoring the RF Spectrum of a Radio

WLAN radios are continually scanning for potential clients. In addition to finding clients, these scans detect other electronic objects, such as other access points and various non-802.11 equipment. (For more information about scanning, see *Understanding Wireless Scanning*.) You can view some of the data collected by the Network Director scanning function by looking at a radio spectrogram in Network Director.

The Network Director radio spectrogram consists of two charts, the Channel Spectrogram on the top half of the screen, and the Spectrum Sweep on the bottom half of the screen.

The Channel Spectrogram displays the selected radio's channel activity, while the Spectrum Sweep displays objects detected in the selected radio's scanned area.

NOTE: **A spectrogram times out after five minutes. During this time, all clients are dropped.**

This topic describes:

Procedure for Viewing the Radio Spectrogram

To view the status of the spectrum:

1. Select **Monitor** Mode in the Network Director banner.
2. Select **Logical View** from the View pane.
3. Expand the list in the View pane, and then select a radio.

TIP: **The Monitor mode RF tab becomes available when you select either an access point or a radio. The RF Spectrogram monitor becomes available only when you select a radio.**

4. Click the **RF** tab.
5. Click **Spectrogram** from the Tasks pane. Two windows open, the RF 2.4-GHz Spectrogram window and the Swept Spectrum and Duty Cycle window.
6. Configure the sweep criteria for the four lines on this chart by adding or deleting the plotted lines. Select or clear the check boxes for Max, Max Hold, Duty Cycle, or Channels. (For an explanation of these values, see Table 26 on page 52.)
7. Click **Start** to begin the sweep using the criteria that you defined.

WARNING: **Your clients are dropped from the selected radio during a sweep.**

8. Sweeps take place in spectral scan mode, which drops all client connections during the sweeps. You are asked if you want to continue. Click **Yes** to drop clients and continue the configured sweeps.

9. The upper graph displays the real-time state of the radio's channels, while the lower graph displays the electronic state of the radio's spectrum. Click **Help** (?) for more information about the graphs or see "Spectrogram Charts" on page 52.
10. When you have seen the desired information, click **Stop**.

    The radio returns to beaconing for potential clients.

Spectrogram Charts

Use the following information to interpret the spectrogram.

The Network Director radio spectrogram consists of charts representing signal strength. On the top half of the screen, the channel power spectrogram for either the 2.4-GHz channel or the 5-GHz channel is displayed. On the lower half of the screen, two tabs display the ongoing spectrum power sweep and the duty cycle sweep.

WARNING: **Your clients are dropped during a spectrum sweep.**

Channel Spectrogram Chart

The channel in use (2.4-GHz or 5-GHz) by the selected radio in the **View** pane is displayed as a grid with these parameters:

- Maximum power
- Average power
- Duty cycle
- Maximum hold

The 2.4-GHz channel has only one tab and all data is plotted on that tab. The larger 5-GHz channel is broken down into tabs for channels: CH-36 to CH-48, CH-52 to CH-64, CH-100 to CH-140, and CH-149 to CH-165. Click each 5-GHz tab to view the individual charts.

Four lines can be plotted on each chart, as listed in Table 26 on page 52:

Table 26: Spectrum Sweep Results

Line	Description
Max Power (red)	Indicates maximum power usage for this radio, plotted at the configured polling interval.
Avg Power (green)	Indicates average power usage for this radio, plotted at the configured polling interval.
Duty Cycle (yellow)	Indicates the amount of RF energy present in the spectrum as a result of an object emitting RF.

Table 26: Spectrum Sweep Results *(continued)*

Line	Description
Max Hold (pink)	Peak power level that was seen across multiple samples.

NOTE: The polling interval can be reconfigured by *Setting Up User and System Preferences*.

You can perform the following actions on this chart:

- Highlight a line in the graph by mousing over the line's legend.
- Display a numeric value by placing the cursor where a vertical grid line bisects a data line.
- Remove any or all of the four lines on this chart by clearing the check boxes for Max, Max Hold, Duty Cycle, or Channels.
- Click **Start** to drop clients and begin the sweep using the criteria that you defined. Click **Stop** to stop the spectrum sweep and return the radios to normal operation.

WARNING: Your clients are dropped during a spectrum sweep.

Swept Spectrum and Duty Cycle Charts

The chart on the bottom half of the window is dynamic, with new sweep results added to the top of the chart after each polling period. The power detected in the sweep is indicated by color, with blue representing the lowest power and red representing the highest power. Typically, the sweep results are blue and green, with occasional yellow segments. Any red that appears in the sweep indicates a problem.

This chart has two tabs, one for average power used in the spectrum called *Swept Spectrum*, and one for the percentage of the *Duty Cycle* used. When you are scanning for either result, all other traffic is dropped. For this reason, you must click **Start** to view spectrum results or see the duty cycle plotted. When you click **Stop**, normal traffic is resumed.

Click the **Swept Spectrum** tab to view the plotted average power spectrum for the radio that you selected in the View pane. The parameters used for this chart are time and average power.

Click the **Duty Cycle** tab to view the duty cycle data for the radio that you selected in the View pane. The parameters used for this chart are time and duty cycle percentage.

This data in these charts is available only for radios.

Related Documentation

- *Understanding Wireless Scanning*

Understanding Wireless Interference

Wi-Fi interference is a common and troublesome issue. The lack of wires that makes WLAN so attractive is also the feature that makes other consumer devices capable of causing Wi-Fi interference. Your WLAN network might be working fine one day and sluggish the next day, without you having made any network changes, all due to interference.

This topic describes:

What Causes Wireless Radio Frequency Interference?

Because the air is shared by all transmitters, transmissions by any device at the same frequency as an access point's radio can cause interference. Because 802.11 wireless networks operate in unlicensed bands used by many technologies, such as microwave ovens, video surveillance cameras, cordless phones, they are subject to interference. In addition, wireless access points sharing the same channel might interfere with each other. The effect of interference is highly dependent on the strength of the transmission and the distance from the interferer. Access points closest to and on the same channel as an interferer will be affected more than those that are further away.

These are some common causes of wireless interference:

- Leaving the channel number on each radio set to the default value can result in high interference among the radios because too many radios are sharing the bandwidth on one channel.
- Hidden nodes in a wireless network referring to nodes that are out of range of other nodes or a collection of nodes. A hidden node can generate a high number of cyclic redundancy check (CRC) code errors.
- Co-channel interference or adjacent channel interference can result from setting radios to bands that have overlapping channels. The channels might not all be in use by your network—neighboring company signals can also cause interference.
- Some non-network devices, such as microwave ovens, car alarms, cordless phones, or wireless video cameras can interfere with wireless channels. Most often, these devices are using the 2.4-GHz frequency.
- Bad electrical connections can cause broad RF spectrum emissions.
- RF jamming is a deliberate attempt to disrupt the network with a powerful signal.

Effects of Interference Seen By Clients

Your network clients might notice the results of interference before you do. They might complain of network slowdown, but not of data loss. This slowdown might not be immediately obvious with low capacity data transmission because, if interference is intermittent, packets eventually get through. Therefore, there is no packet loss, just retransmissions that take time. Another possibility is that some devices, such as microwaves, reduce throughput without blocking it entirely. Complaints will increase when more users log on, increasing data capacity until data loss occurs, or when Voice Over IP calls are placed. VoIP requires significant bandwidth because resending voice is not an option—the result is dropped or jittery voice transmission.

You Can Monitor RF Interference With Network Director

Network Director includes a Monitor Mode that displays the compiled RF data gathered by scanning the mobility domain of your network. There are two monitors that indicate network interference for access points and radios:

- AP Interference Sources—On this chart, interference sources for each radio or each access point (either one can be selected) are sorted into categories such as Microwave Oven, Phone FHSS, and Continuous Wave. The occurrences of each source are tracked and added—the sum appears on a bar chart. The categories with the tallest bars are those causing the most interference on this radio or access point, but the sum of all interference is what really matters. For more information, see "Monitoring RF Interference Sources on Wireless Devices" on page 41.
- Radio Interference Sources—The pie chart for radio interference is also sorted into categories such as Microwave Oven, Phone FHSS, and Continuous Wave. In addition, a list of details are provided about each source of interference—time last seen, transmitter ID, listener MAC address of the access point that found the interference, channel, RSSI, duty cycle, and percentage of compliance to the common information model (CIM). For more information, see "Monitoring RF Interference Sources on One Radio" on page 38.
- RF Interference For Radios on One Access Point—The bar chart that displays each radio on an access point lets you compare the interference experienced on two radios when the access point has dual radios. With single radio access points, you see the same data as you do for the radio interference pie chart, but in bar chart format. For more information, see "Monitoring RF Interference Sources For Radios on One Access Point" on page 38.

What is RF Jamming?

RF jamming is a DoS attack. The goal of RF jamming is to take down an entire WLAN by overwhelming the radio environment with high-power noise. A symptom of an RF jamming attack is excessive interference. If an access point radio detects excessive interference on a channel, and channel auto-tuning is enabled, the radio changes to a different channel. The radio continues to scan on an active data channel and on other channels and reports the results to the controller.

Jamming occurs at the physical layer of the network, saturating the channel or band with noise and making it difficult or impossible for a receiving radio to detect a real transmission. Think of jamming as trying to hear someone talking as a siren goes off. The increased noise floor results in a poor signal-to-noise ratio (SNR), usually detected by the clients as poor signal quality. Jamming can also be detected by an access point, which then triggers dynamic temporary tuning of the channel if automatic channeling is enabled. However, selecting a different channel does not always stop jamming. An experienced attacker will often use all available channels in the attack.

Related Documentation

- Monitoring RF Interference Sources on Wireless Devices on page 41
- Monitoring RF Interference Sources on One Radio on page 38
- Monitoring RF Interference Sources For Radios on One Access Point on page 38
- *Troubleshooting Excessive Wireless Interference*

CHAPTER 6

Monitoring Equipment

Analyzing QFabric Devices

This topic describes how to analyze QFabric devices. The Run Fabric Analyzer task analyzes a QFabric device and provides information about its health, connectivity, and topology.

NOTE: **Fabric analysis is supported for QFabric devices running Junos Release 13.1R2 and higher.**

You must run the Setup QFabric task on the QFabric device to get information about the control plane's health and topology. See *Setting Up QFabrics* for information.

This topic describes:

Procedure for Analyzing a QFabric Device

1. Click **Monitor** in the Network Director banner.
2. Select the QFabric device to analyze in the View pane.
3. In the Tasks pane, select **Tasks** > **Run Fabric Analyzer**.

The results of the analysis appear on the Fabric Analysis tab in Monitor mode, when the QFabric device is selected in the View pane. For information about using the tabs within this tab, see the following sections:

- Using the Fabric Health Check Tab on page 58
- Using the Fabric Connectivity Check Tab on page 58
- Using the Control Plane Topology Tab on page 59
- Using the Data Plane Topology Tab on page 59

Using the Fabric Health Check Tab

To check the health of a QFabric device, select the **Fabric Health Check** tab on the Fabric Analysis tab in Monitor mode. The Fabric Health Check tab contains these sections:

- The Control Plane Health Check section shows information about the health of the QFabric device's control plane. It displays a summary of the control plane health checks performed on the QFabric device. For each summary category, the number of failed (in red) and passed (in green) tests is shown.

  To see detailed information about the tests, click the **Details** button. The Control Plane Health Check Detailed View window opens. This window shows the detailed tests that were performed and their pass/fail status.
- The Data Plane Health Check section shows information about the health of the QFabric device's data plane in a table. Each node device is listed in the Node Device column, and the checks are listed in the other columns.

Using the Fabric Connectivity Check Tab

To check the connectivity of a QFabric device, select the **Connectivity Check** tab on the Fabric Analysis tab in Monitor mode. This tab shows the status of connections between data plane components—Interconnect devices and Node devices. Select which connections to view from the **Show connectivity between** list.

The connectivity check results are shown in a graphical format by default. The connectivity status of each device is color-coded:

- Green—Connected. The software is using all possible physical paths between the two node devices. This is the ideal condition and ensures the best performance given the physical connectivity of the system.
- Red—Not Connected. The software is not using any path between the two node devices, so traffic cannot flow between them.

- Orange—Partially connected. The software is not using all possible physical paths between the two node devices. This might indicate a software error. Traffic should flow smoothly between the two node devices unless so much traffic is sent between the two node devices that all possible paths must be used to prevent packet drops.

You can mouse over a colored square to see the device's name. To see this information in a table, click the table button in the top right portion of the results area.

Using the Control Plane Topology Tab

To see a diagram of the QFabric device's control plane topology, select the **Control Plane Topology** tab on the Fabric Analysis tab in Monitor mode. The link lines are color-coded to indicate the link type. To see the legend for the line color codes, mouse over the button at the top right of the tab. You can zoom in and zoom out of the diagram by using the provided buttons.

Using the Data Plane Topology Tab

To see a diagram of the QFabric device's data plane topology, select the **Data Plane Topology** tab on the Fabric Analysis tab in Monitor mode. You can zoom in and zoom out of the diagram by using the provided buttons.

Related Documentation

- Understanding the Monitor Mode Tasks Pane on page 11

Comparing Device Statistics

This topic describes how to compare statistics from multiple network devices and interfaces in real time. You select which devices, interfaces, and counters to compare, and how often to poll for new statistics.

This topic describes:

Procedure for Comparing Device Statistics

1. Click **Monitor** in the Network Director banner.

   You can compare device statistics in any tab in Monitor mode.

2. In the Tasks pane, select **Tasks** > **Compare Device Statistics**.

   The Compare Interfaces window opens. For information about this window, click the Help button in the title bar of the window or see "Compare Interfaces Window" on page 59.

Compare Interfaces Window

The Compare Interfaces window enables you to compare statistics from multiple device interfaces in real time. The search scope is the entire managed network, regardless of which node is selected in the View pane.

To compare device statistics:

1. Select the devices to compare from the device tree in the Select Devices section.
2. Select a device in the Selected Devices section to select which of its interfaces to compare.

   The Select Interfaces section lists the device's interfaces. You can select up to two interfaces per device.
3. Select an Interface in the Select Interfaces section to select which of its counters to compare.

   The Select Counters section lists the interface's counters.
4. Select the counters to compare in the Select Counters section.
5. Repeat the process of selecting devices, interfaces, and counters to compare until you are finished selecting what to compare.
6. Select how often the data will be refreshed from the **Data Collection Frequency** list.
7. Click the **Compare** button to start comparing information.

   A page opens containing a line graph for each counter you selected. Each graph displays all the interfaces for which its counter is selected.
8. To pause data collection, click the **Pause** button. To resume data collection, click the **Resume** button.
9. To change data collection settings, click the **Back** button.

Related Documentation

- Understanding the Monitor Mode Tasks Pane on page 11

Monitoring Backed-Up Wireless Access Points on Wireless LAN Controllers

This topic describes how to monitor backed-up wireless access points on a wireless LAN controller. You can monitor backed-up wireless access points on wireless LAN controller nodes in any view.

When wireless LAN controllers are configured in a cluster, each wireless access point in the cluster can have a primary controller and a secondary controller. You can see which wireless access points use the selected wireless LAN controller as their secondary controller. The term backed-up means that the wireless LAN controller is acting as a secondary (backup) controller for a wireless access point.

This topic describes:

- Procedure for Monitoring Backed-Up Wireless Access Points on Wireless LAN Controllers on page 61
- Backed-Up APs Window on page 61

Procedure for Monitoring Backed-Up Wireless Access Points on Wireless LAN Controllers

1. Click **Monitor** in the Network Director banner.
2. Select the wireless LAN controller in the View pane that contains the backed-up wireless access points you want to monitor.
3. Select the **Summary** tab or the **Equipment** tab.
4. In the Tasks pane, select **View** > **Backed-Up APs**.

   The Backed-Up APs window opens. For information about this window, click the Help button in the title bar of the window or see "Backed-Up APs Window" on page 61.

Backed-Up APs Window

The Backed-Up APs window contains a table with information about the backed-up wireless access points on the node you selected in the View pane. See Table 27 on page 61 for a description of the table information.

Table 27: Backed-Up APs Table

Table Column	Description
AP Name	Name of the access point.
Serial Number	Serial number of the access point.
Model	The model number of the access point.
IP Address	The IP address assigned to the AP.
Status	Operational status of the access point: • Down—The access point is offline. • Up—The access point is online and enabled. • Up Redundant—The access point is online, reporting to this controller as redundant and another controller as primary.
Uptime	The length of time since the access point last booted.
Version	The version of the Mobility System Software (MSS) running on the access point.
Primary Controller	The primary controller for the access point.
Secondary Controller	The secondary controller for the access point.

Related Documentation

- Understanding the Monitor Mode Tasks Pane on page 11

Monitoring QFabric Devices and Components

This topic describes how to monitor QFabric devices and their components, and which QFabric-specific monitors are available.

To monitor a QFabric device or its components:

1. Click **Monitor** in the Network Director banner.
2. Select a QFabric device node or a node within a QFabric device node that you want to monitor in the View pane.

   The tabs and monitors that are available depend on the type of node you select.
3. To get information about a monitor, click the Help button in its title bar, or refer to Table 28 on page 62 for information about the QFabric-specific monitors that are available for each node type.

Table 28: Monitors Available for QFabric Devices and Components

QFabric Node Type Selected in the View Pane	Monitoring Tab	Available QFabric-Specific Monitors
QFabric device	Summary	• Status Monitor for QFabrics on page 105 • Access vs. Uplink Port Utilization Trend Monitor on page 77 • Node Device Summary Monitor on page 85 • QFabric Interconnect Status Summary Monitor on page 89
	Equipment	"Status Monitor for QFabrics" on page 105
	Fabric Analysis	For information about fabric analysis, see "Analyzing QFabric Devices" on page 57.
Directors folder	Summary	"QFabric Director Status Monitor" on page 89
Director device	Summary	• Status Monitor for QFabric Directors on page 103 • QFabric VM Status Summary Monitor on page 90
Interconnects folder	Summary	"QFabric Interconnect Status Summary Monitor" on page 89
Interconnect device	Equipment	"Status Monitor for QFabric Interconnects" on page 104
Node Group folder (applies to Server, Redundant Server, and Network Node Groups)	Summary	"Node Device Summary Monitor" on page 85
Node Group (applies to Server, Redundant Server, and Network Node Groups)	Summary	"Node Device Summary Monitor" on page 85
Node device (applies to Server, Redundant Server, and Network Nodes)	Summary	"Access vs. Uplink Port Utilization Trend Monitor" on page 77
	Equipment	"Status Monitor for QFabric Nodes" on page 104

Related Documentation

- Understanding Monitor Mode in Network Director on page 3

Monitoring the Status of Aggregated Access Points and Radios

Network Director provides two monitors that display an aggregate view of access points and radios at the network level. Aggregation is available for Controller Clusters, Wireless Mobility Domains, and the Wireless Network.

To locate these monitors:

1. Click **Monitor** in the Network Director banner to ensure that you are in Monitor mode. Monitor mode works in all views (Logical, Location, Device).
2. Select a supported node in the network tree (**Wireless Network**, **Wireless Mobility Domain**, or**Controller Cluster**). The Equipment tab is the default tab that displays the AP Status and Radio Status.
3. Click the Help icon on the monitor to learn more about the purpose or fields on a monitor.

The two monitors that display aggregate information for APs and Radios are:

- "AP Status Monitor" on page 77, summarizes of all of the network access points
- "Radio Status Monitor" on page 90, summarizes of all of the network radios

Related Documentation

- AP Status Monitor on page 77
- Radio Status Monitor on page 90

Monitoring the Status of Logical Interfaces

Network Director provides real-time statistics on logical Ethernet switching interfaces for switches and Virtual Chassis. These statistics are available in Monitoring mode when one of these device nodes is selected in any view.

This topic describes:

- Locating Information about Logical Interfaces on page 63
- Show Logical Interface Information Table on page 64

Locating Information about Logical Interfaces

Real-time logical interface statistics, including VLAN information are available from the Show Logical Interfaces window in Monitoring mode. To find this information:

1. Select **Monitor** in the Network Director banner.
2. Select a switch or Virtual Chassis from the network tree in any view.

3. Select the Equipment tab.
4. Click **Logical Interfaces** in the Tasks pane to open the Show Logical Interface Information table in main window.

Show Logical Interface Information Table

The Show Logical Interface Information table provides interface, VLAN, and spanning-tree status for an interface. The information is presented in a tabular format. The fields in the Show Logical Interface Information window are describes in Table 29 on page 64.

Scope information: This task window is available from the Tasks pane when you select a switch or Virtual Chassis in any view.

Table 29: Show Logical Interface Information Fields

Field	Description
Logical Interface Name	The logical interface name.
VLAN Membership ID	The VLAN which the interface belongs.
802.1Q Tag	The IEEE 802.10 identifier for the VLAN.
Tagging	Indicates whether the packets entering the port are tagged or untagged.
Logical Interface State	Indicates whether the logical interface is up or down.
STP State	Indicates whether the interface is blocking or forwarding (unblocked).
Port Mode	Indicates one of three modes: access, tagged-access, or trunk. • Access—The interface can be in a single VLAN only. • Tagged-access—The interface can accept tagged packets from one access device. • Trunk—The interface can be in multiple VLANs and accept tagged packets from multiple devices.

Related Documentation

- Monitoring Traffic on Devices on page 21
- Monitoring Traffic on Layer 3 VLANs on page 26

Monitoring the Status of Standalone Switches

When you select a switch from the network tree in any view, a dashboard comprising four monitors display that give at-a-glance information about the status and performance information of the switch.

To locate the monitors for switches:

1. Click **Monitor** in the Network Director banner to ensure that you are in Monitor mode.
2. Expand the network tree to expose the switch node.

3. Select the switch in the network tree.
4. Click the **Equipment** tab to expose the four monitors and to update the tasks that are available for the switch.

The four monitors are:

- "Resource Utilization Monitor for Switches and Virtual Chassis" on page 91, that provides a graphical representation of CPU usage and memory consumption.
- "Status Monitor for Switches" on page 105, that provides information about the uptime, IP address, and hostname of the switch.
- "Port Status Monitor" on page 86, that provides port level status information.
- "Power Supply and Fan Status Monitor" on page 88, that provides a graphical representation of the operating condition for the units. These graphs also show the ratio of filled slots to available power and fan bays.

Related Documentation

- Understanding Monitor Mode in Network Director on page 3
- Resource Utilization Monitor for Switches and Virtual Chassis on page 91
- Status Monitor for Switches on page 105
- Port Status Monitor on page 86
- Power Supply and Fan Status Monitor on page 88

Monitoring the Status of a Virtual Chassis

When you select a Virtual Chassis from the network tree in any view, four monitors are displayed that give at-a-glance information about the status and performance of the Virtual Chassis. Use this information to monitor the chassis as a whole, without reviewing each switch independently.

To locate the Virtual Chassis monitors:

1. Click **Monitor** in the Network Director banner to ensure that you are in Monitor mode.
2. Expand the network tree to expose the Virtual Chassis node.
3. Select the Virtual Chassis in the network tree.
4. Click the **Equipment** tab to display the four monitors.
5. Click the Help icon on the monitor learn more about the purpose or fields on a monitor.

The four monitors are:

- "Resource Utilization Monitor for Switches and Virtual Chassis" on page 91, that provides information about the composition of the chassis, its members, and the location of neighboring switches.
- "Status Monitor for Virtual Chassis" on page 107, that provides information about the uptime, IP address, and hostname of the Virtual Chassis.

- "Resource Monitor For Wireless LAN Controllers" on page 92, that provides a graphical representation of CPU usage and memory consumption.
- "Port Status Monitor" on page 86, that provides port level status information.

Related Documentation

- Monitoring the Status of Virtual Chassis Members on page 66
- Resource Utilization Monitor for Switches and Virtual Chassis on page 91
- Status Monitor for Virtual Chassis on page 107
- Resource Monitor For Wireless LAN Controllers on page 92
- Port Status Monitor on page 86

Monitoring the Status of Virtual Chassis Members

When you select a member of a Virtual Chassis in the any view, Network Director displays four monitors. At the member node level, the information is highly specific to the equipment.

To locate these monitors:

1. Click **Monitor** in the Network Director banner to ensure that you are in Monitor mode.
2. Expand the network tree to expose the member of the Virtual Chassis node.
3. Select the Virtual Chassis in the network tree.
4. Click the **Equipment** tab to display the monitors.
5. Click the Help icon on the monitor to learn more about the purpose or fields on a monitor.

The monitors at this level are:

- "Port Status Monitor" on page 86, that provides summary and detailed information about the status of the physical network interfaces for the selected node in the View pane.
- "Power Supply and Fan Status Monitor" on page 88, that provides a graphical representation of the operating condition for this member. These graphs also show the ratio of filled slots to available power and fan slots.
- "Status Monitor for Virtual Chassis Members" on page 108, that provides status information for this member of the Virtual Chassis.

Related Documentation

- Monitoring the Status of a Virtual Chassis on page 65
- Port Status Monitor on page 86
- Power Supply and Fan Status Monitor on page 88
- Status Monitor for Virtual Chassis Members on page 108

Monitoring the Status of Wireless Controllers, Access Points, and Radios

When you select the node of a wireless controller in any view, Network Director presents four monitors. These monitors give you the overall workload and performance of the controller and the APs and radios under its control.

To locate the monitors that are specific to wireless controllers:

1. Click **Monitor** in the Network Director banner to ensure that you are in Monitor mode..
2. Expand the network tree to expose the wireless controller.
3. Select the wireless controller.
4. Click the **Equipment** tab. The page opens with the four monitors.

The available monitors are:

- "Resource Monitor For Wireless LAN Controllers" on page 92, that provides a graphical representation of CPU usage and memory consumption.
- "Equipment Status Summary Monitor" on page 83, that provides state information on ports, access points and radios.
- "AP Status Monitor" on page 77, that provides details of each AP including the current uptime.
- "Radio Status Monitor" on page 90, that provides details of each radio under the controller's control.

Related Documentation

- Resource Monitor For Wireless LAN Controllers on page 92
- Equipment Status Summary Monitor on page 83
- AP Status Monitor on page 77
- Radio Status Monitor on page 90

CHAPTER 7

Monitoring Virtual Devices

Using Monitor Mode for Virtual Devices

The Monitor mode for virtual devices in your network enables you to view details about your virtual network using the following tabs:

- Summary—Displays the status of the virtual network, virtual machine, or virtual switch, active alarms, and the number of hosts and the version of VMware ESXi that is running on each host.
- vMotion History—vSphere vMotion is a feature that enables live migration of running virtual machines from one host to another with zero downtime and continuous network availability. You can view the status of the history of all the vMotions for your virtual network in the vMotion History tab. For more details, see "Viewing vMotion History in Network Director" on page 72.

Your current scope—that is, your view and node selection in the View pane—affects which Monitor widgets are available. For example, if you select a virtual switch, Network Director displays the status and the active alarms for the selected virtual switch.

This topic describes:

Current Active Alarms Monitor

The Current Active Alarms monitor shows any active alarm that has not yet been cleared. It is one of the four standard monitors available in Alarm mode. Current Active Alarms is a table that has four fields and appear by default. However, nine fields are available for selection. See Table 30 on page 70 for a description of the table.

Table 30: Current Active Alarms Monitor

Table Column	Description	Shown in Summary by Default	Shown in Detailed View by Default
Name	The alarm name.	Yes	Yes
ID	A system and sequentially-generated identification number.	No	No
Assigned To	If assigned to an individual, it shows the name of the person assigned; otherwise, it shows System to mark that the alarm is still unassigned.	No	Yes
Severity	The severity of the alarm. Severity levels are: • Critical—A critical condition exists; immediate action is necessary. • Major—A major error has occurred; escalate or notify as necessary. • Minor—A minor error has occurred; notify or monitor the condition. • Info—An informational message; no action is necessary.	Yes	Yes
Entity ID	The identification of the entity responsible for causing this alarm. The Entity ID is the key for correlation of events into an alarm. The Entity ID could be a MAC address of a radio or an IP address of the device.	Yes	Yes
Source	The IP address of the device or network element that generated the alarm. The SNMP agent is located at the source IP. In most cases, the source IP is the IP address of the switch or controller.	No	No
Reporting Device	The hostname or IP address of the reporting device.	Yes	Yes
Creation Date	The date and time the alarm was first reported.	No	No
Last Updated	The date and time that the information for the alarm was last modified.	Yes	Yes
Updated By	Either the system or the last user who modified the alarm.	No	No

Clicking the Details icon opens Alarm Details where you can sort and disposition alarms by state (Acknowledged, Clear, Active).

Status Monitor

This monitor provides key information about the status for the virtual device selected in the Virtual view. This monitor is on the Summary tab in Monitor mode.

Table 31 on page 71 describes the fields in this monitor.

Table 31: Status Monitor Fields

Field	Function	Scope
Name	The hostname of the virtual device.	All
Hardware	The hardware platform that the host uses.	Host
Connection Status	The connection status of the host and the virtual machines.	Host
Hypervisor	The version of VMware ESXi that is installed on the host.	Host
Number of Virtual Switches	The number of virtual switches available for the selected scope.	Virtual Network, Host
Number of Virtual Machines	The number of virtual machines available for the selected scope.	All
Sync Status	Indicates if the virtual network configuration is synchronized with Network Director.	Virtual Network
Orchestration Status	Displays the orchestration status of the virtual network.	Virtual Network
MTU	The maximum size of a protocol data unit that can be transmitted using the virtual switch.	Virtual Switch
Number of Port Groups	The number of port groups that are defined for the selected virtual switch. Port group is a template that stores a set of configuration that is used to create virtual switch ports on a virtual switch.	Virtual Switch

Host Count Summary By Version

To view Host Count Summary By Version widget, you must select Hosts from the View pane while you are in the Virtual view with Monitor mode selected.

The Host Count by Summary widget displays the hosts and the VMware ESXi version that is installed on each host, using a pie chart. Mouse over a pie segment to view the actual number of devices and the percentage represented by that pie segment.

Virtual Switch Summary By Version

To view Virtual Switch Summary By Version widget, you must select Virtual Switches from the View pane while you are in the Virtual view with Monitor mode selected.

The Virtual Switch Summary By Version displays the standard and distributed switch, and the software version that is installed on the switch, using a pie chart. Mouse over a pie segment to view the actual number of devices and the percentage represented by that pie segment.

Related Documentation

- Viewing vMotion History in Network Director on page 72

Viewing vMotion History in Network Director

vSphere vMotion is a feature that enables live migration of running virtual machines from one host to another with zero downtime and continuous network availability. vMotion is a key feature that enables the creation of a dynamic, automated and self-optimizing datacenter.

If a vMotion happens in any of the virtual machines that are under the management of Network Director, then Network Director initiates a job to track the vMotion and the corresponding changes to orchestration. You can view the status of the history of all the vMotions for your virtual network in the vMotion History page. You can also view the status of the orchestration job that is initiated due to this vMotion by clicking on the Orchestration Job ID field.

After the orchestration job is completed successfully, you must manually resynchronize the physical switch's configuration with Network Director. If the system of record (SOR) mode set for the Junos Space Network Management Platform is:

- Network as system of record (NSOR), then performing a resynchronization ensures that Junos Space automatically resynchronizes its configuration record to match the device configuration and sets the device configuration state to In Sync when the synchronization completes. For more details, see *Resynchronizing Device Configuration*.
- Junos Space as system of record (SSOR), then you must perform a resynchronization and accept the out-of-band changes. Both the Junos Space configuration record and the Network Director Build mode configuration are resynchronized to reflect the out-of-band configuration changes. For more details, see *Resynchronizing Device Configuration*

To view the vMotion history:

1. While in the Monitor mode, select a Virtual Network.
2. Select the **vMotion History** tab.

   The vMotion History page appears. You can view the details shown in Table 32 on page 72 in the vMotion History page.

Table 32: View vMotion History fields

Field	Description
VM Name	Name of the virtual machine that had undergone a vMotion.
vNetwork	Name of the virtual network.
Source Host	The host from which the virtual machine moved.
Destination Host	The host to which the virtual machine moved.
Started On	Time when the vMotion started.

Table 32: View vMotion History fields *(continued)*

Field	Description
Completed On	Time when the vMotion completed.
Status	Indicates the status of the vMotion.
Source Switches	Host name of the physical switch to which the host was connected before the vMotion.
Source Switch Port	Port on the source physical switch to which the host was connected.
Destination Switches	Host name of the physical switch to which the host is connected after the vMotion.
Destination Switch Port	Port on the destination physical switch to which the host is connected.
Orchestration Job IDs	The ID of orchestration job that was initiated as a result of the given vMotion. You can click on a job ID to view details about the orchestration job that got initiated as a result of the vMotion.
MAC Address	MAC address of the virtual machine.

3. You can check the status of the orchestration job corresponding to a given vMotion by clicking on the orchestration job ID. Network Director opens the vMotion Orchestration window displaying job details such as the name, percentage complete, status, start and end time, and the summary of the job.

Related Documentation

- *Understanding Virtual Network Management*

CHAPTER 8

Monitor Reference

802.11 Packet Errors Monitor

The 802.11 Packet Errors monitor displays the number of packet errors experienced by the object selected in the View pane. The object is polled and plotted at the standard polling rate.

You can perform the following actions on this graph:

- Change the time period over which to display the percentage of retransmitted packets by selecting a time period from the list in the upper right corner.
- Display a numeric value by mousing the cursor where a vertical grid line bisects a data line.

Packet error data is available when you select a radio, an access point, a floor, a building, or a site in any view. Radios and access points are displayed automatically in the View pane—you must configure floors, buildings, and sites. See *Creating a Site*, *Configuring Buildings*, and *Configuring Floors* for details.

If your packet error rate is too high, you can try to lower it by:

- Locating and eliminating noise that could be causing causes spurious packets. For more information about noise, see "Monitoring RF Interference Sources on Wireless Devices" on page 41, "Monitoring RF Interference Sources on One Radio" on page 38, and "Monitoring RF Interference Sources For Radios on One Access Point" on page 38.
- Checking for weak signals. If automatic power tuning is not enabled, try enabling it. For more information, see *Understanding Automatic Power Tuning for Wireless Radios*.
- Assigning access points to different channels. When channels are too congested, packet collision and corruption can occur. If automatic channel tuning is not enabled, try enabling it. For more information, see *Understanding Wireless Radio Channels* and *Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks*.

Related Documentation

- Monitoring RF 802.11 Packet Errors on page 36
- *Creating a Site*

- *Configuring Buildings*
- *Configuring Floors*
- Monitoring RF Interference Sources on Wireless Devices on page 41
- Monitoring RF Interference Sources on One Radio on page 38
- Monitoring RF Interference Sources For Radios on One Access Point on page 38
- *Understanding Automatic Power Tuning for Wireless Radios*
- *Understanding Wireless Radio Channels*
- *Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks*

Access vs. Uplink Port Utilization Trend Monitor

The Access vs. Uplink Port Utilization Trend monitor shows trends in the bandwidth utilization of access and uplink ports within the selected QFabric device or node device. It is available on the Summary tab in Monitor mode.

NOTE: **After a device is discovered, trend data does not appear immediately—it appears only after three polling periods have occurred.**

The information is shown in a line graph. The vertical axis shows bandwidth utilization percentage. The horizontal axis shows the times when data was polled. At each poll, the bandwidth utilization percentage of each port type (access and uplink) is indicated by a dot. The dots are connected by lines to show the trend over time.

You can perform the following actions on the line graph:

- Change the time period over which to display the traffic trends by selecting a time period from the list in the upper right corner.
- Highlight a line in the graph by mousing over the line's legend.
- Remove or restore a line by clicking its legend.
- Display a numeric value by mousing over where a vertical grid line crosses a data line.

Related Documentation

- Understanding Monitor Mode in Network Director on page 3

AP Status Monitor

The AP Status monitor displays status information about all access points that belong to the selected node. It is found on the Equipment tab in Monitor mode.

The default view of the summary shows four of the eight available fields that you can configure to be shown or hidden. The details page shows an expanded version with all of the fields, which can also be tailored.

This monitor currently displays for the top wireless node and for wireless LAN controller nodes. If, for example, you select Wireless Network node, it shows global status information for all access points. If you select a wireless LAN controller, it shows status information for the access points belonging to the controller.

Table 33 on page 78 describes the fields that are available in both the summary and detail view of the AP Status monitor. Fields that are available, but hidden, are also displayed.

Table 33: AP Status Monitor Fields

Field	Description	Summary, Detailed, or Hidden View
AP Name	Name of the access point.	Summary
Serial Number	Serial number of the access point.	Summary
Model	The model number of the access point.	Summary (hidden) Detailed
IP Address	The IP address assigned to the AP.	Summary (hidden) Detailed
Status	Operational status of the access point: • Down—The access point is offline. • Up—The access point is online and enabled. • Up Redundant—The access point is online, reporting to this controller as redundant and another controller as primary.	Summary
Uptime	The length of time since the access point last booted.	Summary
Version	The version of the Mobility System Software (MSS) running on the access point.	Summary (hidden) Detailed
Controller Name	The primary controller for the access point.	Summary (hidden)
Primary Controller	The primary controller for the access point.	Detailed
Secondary Controller	The secondary controller for the access point.	Detailed

Related Documentation

- Monitoring the Status of Aggregated Access Points and Radios on page 63
- Monitoring the Status of Wireless Controllers, Access Points, and Radios on page 67

- *Device Inventory Report*

Current Sessions Monitor

The Current Sessions monitor provides summary and detailed information about the active sessions within the node selected in the View pane. This monitor is available in the Client tab.

- Current Sessions on page 79
- Current Sessions Details on page 79

Current Sessions

The summary view of the Current Sessions monitor displays a graph of the number of active sessions within the node selected in the View pane.

Current Sessions Details

The User Session Details window contains a table with detailed information about the active sessions within the current node selected in the View pane.

The following table describes the columns that appear in the current session details table.

Table 34: Current Session Details Table

Table Column	Description
User Name	Client's user name
MAC Address	Client's MAC address.
Device Type	Client's device type.
Device Group	Client's device group.
Device Profile	Client's device profile.
Controller IP	IP address of the controller to which the client is connected.
AP ID	ID of the wireless access point to which the client is connected.
AP NAME	Name of the wireless access point to which the client is connected.
SSID	SSID to which a wireless client is connected.
VLAN	VLAN to which the client is connected.
Client IP	Client's IP address.
Auth Type	Authorization type used for the client.

Table 34: Current Session Details Table *(continued)*

Table Column	Description
B/w[KBps]	Bandwidth used by the client.
Node Name	Client's node name.
Data Usage (KBytes)	Data transmitted and received by the client, in kilobytes.
Elapsed Time	Length of time the session has been active.
Sample Time	Time when the most recent sample was taken.

TIP: Some table columns are hidden by default. To select which columns to display, mouse over any column heading, click the arrow that appears, mouse over **Columns** in drop-down menu, and then select the columns to display from the list.

Related Documentation

- Monitoring Client Sessions on page 29

Current Sessions by Type Monitor

The Current Sessions by Type monitor provides summary and detailed information about the active sessions within the node selected in the View pane. This monitor is available in the Client tab.

- Current Sessions on page 80
- Current Sessions Details on page 80

Current Sessions

The summary view of the Current Sessions by Type monitor shows a pie chart of the active sessions within the node selected in the View pane. The chart shows the distribution of sessions by the session type. To change the session type shown in the monitor, select from the **Choose Sessions By Type** list.

Current Sessions Details

The User Session Details window contains a table with detailed information about the active sessions within the current node selected in the View pane.

The following table describes the columns that appear in current session details tables.

Table 35: Current Session Details Table

Table Column	Description
User Name	Client's user name

Table 35: Current Session Details Table *(continued)*

Table Column	Description
MAC Address	Client's MAC address.
Device Type	Client's device type.
Device Group	Client's device group.
Device Profile	Client's device profile.
Controller IP	IP address of the controller to which the client is connected.
AP ID	ID of the wireless access point to which the client is connected.
AP NAME	Name of the wireless access point to which the client is connected.
SSID	SSID to which a wireless client is connected.
VLAN	VLAN to which the client is connected.
Client IP	Client's IP address.
Auth Type	Authorization type used for the client.
B/w[KBps]	Bandwidth used by the client.
Node Name	Client's node name.
Data Usage (KBytes)	Data transmitted and received by the client, in kilobytes.
Elapsed Time	Length of time the session has been active.
Sample Time	Time when the most recent sample was taken.

Not all table columns are visible by default. To select which columns to display, mouse over any column heading, click the arrow that appears, mouse over **Columns** in drop-down menu, then select the columns to display from the list.

Related Documentation

- Monitoring Client Sessions on page 29

Error Trend Monitor

The Error Trend monitor displays inbound and outbound error trends on the node you selected in the View pane. This monitor is available in the Traffic tab.

This topic describes:

Error Trend

A line graph shows the rate inbound and outbound errors over time. The horizontal axis shows the times when samples were taken. The vertical axis shows errors.

NOTE: **After a device is discovered, trend data does not appear immediately—it appears only after three polling periods have elapsed.**

You can perform the following actions on the line graph:

- Change the time period over which to display the traffic trends by selecting a time period from the list in the upper right corner.
- Highlight a line in the graph by mousing over the line's legend.
- Remove or restore a line by clicking its legend.
- Display a numeric value by mousing over where a vertical grid line crosses a data line.

Error Trend Details

The Error Trend details window displays detailed information about the top users within the node you selected in the View pane. It contains the following elements:

- A line graph shows the rate of errors over time. The horizontal axis shows the times when samples were taken. The vertical axis shows errors.

  NOTE: **After a device is discovered, trend data does not appear immediately—it appears only after three polling periods have elapsed.**

  You can perform the following actions on the line graph:

  - Change the time period over which to display the traffic trends by selecting a time period from the list in the upper right corner.
  - Highlight a line in the graph by mousing over the line's legend.
  - Remove or restore a line by clicking its legend.
  - Display a numeric value by mousing over where a vertical grid line crosses a data line.

- Error Trend Details table—Shows detailed information about the data gathered at each sample. For information about this table, see Table 36 on page 83

- Error Trend Additional Details table—Shows Additional error trend details and allows you to display them on the graph. For information about this table, see Table 37 on page 83.

Table 36: Error Trend Details Table

Column	Description
Time	Time when a data sample was taken from devices.
Errors In	Number of inbound errors reported in the sample.
Errors Out	Number of outbound errors reported in the sample.
CRC Errors In	Number of inbound cyclic redundancy check (CRC) errors reported in the sample.
CRC Errors Out	Number of inbound CRC errors reported in the sample.

Table 37: Error Trend Additional Details Table

Column	Description
Series Name	Name of the data series.
Series Value	Value of the data series.
Show	Select the check box to display the series on the graph. Deselect the check box to remove it from the graph.

Related Documentation

- Monitoring Traffic on Devices on page 21

Equipment Status Summary Monitor

The Equipment Status Summary monitor provides status highlights for the wireless controller ports, access points, and radios in the current scope. Both the summary and details show up to five available fields. Table 38 on page 83 describes the fields in this monitor.

Table 38: Equipment Status Summary Fields

Field	Function	Default View
Device	Indicates the type of device being run by the wireless controller: access points, radios, and ports.	Summary Details
Up	Indicates how many of the devices are up.	Summary Details
Down	Indicates how many of the devices are down.	Summary Details

Table 38: Equipment Status Summary Fields *(continued)*

Field	Function	Default View
Unknown	Indicates if the controller cannot identify the device.	Summary Details
Disabled	Indicates if the device is disabled.	Summary Details

Related Documentation

- Monitoring the Status of Wireless Controllers, Access Points, and Radios on page 67
- AP Status Monitor on page 77
- Radio Status Monitor on page 90

Equipment Summary By Type Monitor

The Equipment Summary By Type monitor provides summary and detailed information about the type and number of devices in the scope selected in the View pane. This monitor is available on the Summary tab in Monitor mode.

Equipment Summary By Type

The summary view of the Equipment Summary By Type monitor shows the distribution of device types in the selected scope. Switches in a Virtual Chassis are counted separately from standalone switches.

Mouse over a segment of the pie chart to see the actual number of devices of that type. Click the details icon to open the Equipment Summary By Type Detail View window.

Equipment Summary By Type Details

The Equipment Summary By Type Detail View window provides details about the distribution of device types in the selected scope. Each table row represents a device type. Device types are defined by the combination of a device family, platform, and operating system version (for some device types). See Table 39 on page 84 for a description of the table columns.

Table 39: Equipment Summary By Type Detail View

Table Column	Description
Device Family	Device family.
Platform	Device platform.
OS Version	Operating system version running on the device.
Device Type	Device type.
Count	Number of devices of this platform in the selected scope.

Related Documentation

- Selecting Monitors To Display on the Summary Tab on page 19

Node Device Summary Monitor

The Node Device Summary monitor displays information about the port utilization of the nodes within the selected QFabric fabric or container within a fabric. It is on the Summary tab in Monitor mode. The information is presented in a bar chart. The vertical axis shows node names. The horizontal axis shows the number of ports. Ports are categorized based on the percentage of allocated bandwidth they use: over 80%, between 50-80%, and below 50%. The bar color codes for the categories are shown in the legend below the chart. The five nodes that are using the highest percentage of their bandwidth are shown on the monitor.

Related Documentation

- Understanding Monitor Mode in Network Director on page 3

Percentage of Packets Retransmitted Monitor

The Percentage of Packets Retransmitted monitor displays the percentage of wireless data packet retransmissions experienced by the access point or radio selected in the Network Director View pane.

You can perform the following actions on this line graph:

- Change the time period over which to display the percentage of retransmitted packets by selecting a time period from the list in the upper right corner.
- Display a numeric value by placing the cursor where a vertical grid line bisects a data line.

Ideally, packet retransmission does not exceed 10% of the total number of packets sent. If your retransmission percentage is higher, you can try to lower it by:

- Locating and eliminating noise that could be causing causes spurious packets. For more information on noise, see "Monitoring RF Interference Sources on Wireless Devices" on page 41, "Monitoring RF Interference Sources on One Radio" on page 38, and "Monitoring RF Interference Sources For Radios on One Access Point" on page 38.
- Checking for weak signals. Automatic power tuning will help improve weak signals. For more information, see *Understanding Automatic Power Tuning for Wireless Radios*.
- Assigning access points to different channels. When channels are too congested, packet collision and corruption can occur. Enable automatic channel tuning enabled if it is not already enabled. For more information, see *Understanding Wireless Radio Channels* and *Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks*.

  Retransmitted packet data is available when you either select a radio or an access point.

Related Documentation

- Monitoring RF Interference Sources on Wireless Devices on page 41
- Monitoring RF Interference Sources on One Radio on page 38
- Monitoring RF Interference Sources For Radios on One Access Point on page 38
- *Understanding Automatic Power Tuning for Wireless Radios*
- *Understanding Wireless Radio Channels*
- *Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks*

Port Status Monitor

The Port Status monitor provides summary and detailed information about the status of the physical network interfaces for the selected node in the View pane.

This monitor is available in the Equipment tab of Monitor mode when you select an EX Series switch or Virtual Chassis member in any view. For individual devices, it displays port information specific to the device. However on the Summary tab, it displays aggregated data from all switches and Virtual Chassis in the network.

This topic describes:

Port Status Summary

The summary view of the Port Status monitor displays two pie charts:

- Admin Status–Of the interfaces on the selected node, shows the proportion of interfaces that are administratively enabled and that are administratively disabled.
- Free vs Used–Of the network interfaces that are administratively enabled, shows the proportion of interfaces that are in use (operationally up) and that are not in use (operationally down).

Mouse over a pie segment to view the actual number of ports. Click the details icon to open the Port Status Details window.

Port Status Details

The Port Status Details table provides details about the physical network interfaces for the selected node, as shown in Table 40 on page 87.

NOTE: **You must have a transceiver plugged into an SFP, SFP+, or XFP port for information about the port to appear.**

Table 40: Port Status Details

Field	Description
Port Name	The name of the physical interface.
MAC Address	For standalone EX Series switches, the first five groups of hexadecimal digits are determined when the switch is manufactured. The switch then assigns a unique MAC address to each interface by assigning a unique identifier as the last group of hexadecimal digits. For Virtual Chassis members, the first four groups of hexadecimal digits are determined when the switch is manufactured. The fifth group of hexadecimal digits reflects the role of the member in the chassis, such as master or line card.
Serial Number	The hardware serial number of the device.
Host Name	The hostname of the device.
Description	A text description of the physical interface.
Speed (Mbps)	The speed of the port, in megabits per second (Mbps).
Duplex Mode	The duplex mode: full (full-duplex), half (half-duplex), or auto (autonegotiation).
Port Type	For EX Series switches, the port type can be 1 Gigabit Ethernet or 10 Gigabit Ethernet interface.
Admin Status	The administrative state of the port: enabled (up) or disabled (down).
Operational Status	The operational status: link up or link down.
Last Flap Time	Date and time at which the advertised link became unavailable, and then, available again.

Related Documentation

- Monitoring the Status of Virtual Chassis Members on page 66
- Monitoring the Status of Standalone Switches on page 64

Port Utilization Monitor

The Port Utilization monitor displays a bar chart with information about the port traffic utilization on the node you selected in the View pane. This monitor is available on the Summary tab in Monitor mode. Each bar in the chart represents the port traffic utilization data gathered at a polling interval. The vertical axis shows the number of ports polled. The horizontal axis shows the time when each poll was taken.

Each bar is divided into the following colored sections to indicate the distribution of port traffic utilization at the polling interval:

- Green indicates ports that operated at less than 50% of negotiated speed.
- Orange indicates ports that operated at between 50% and 80% of negotiated speed.

- Red indicates ports that operated at more than 80% of negotiated speed.

You can perform the following actions on the bar chart:

- Change the time period over which to display the data by selecting a time period from the list in the upper right corner.
- Remove or restore a utilization category (bar color) by clicking its legend.
- Display a numeric value by mousing over a bar.

Related Documentation

- Monitoring Traffic on Devices on page 21

Power Supply and Fan Status Monitor

The Power Supply and Fan monitor provides information about the availability and status of switch power supplies and cooling fans for the node you select in the View pane.

This monitor is available when you select an EX Series switch or a Virtual Chassis member in any view. It appears on the Equipment tab when in Monitor mode.

This topic describes:

- Power Supply and Fan Status on page 88
- Power Supply and Fan Status Details on page 88

Power Supply and Fan Status

The summary view of the Power Supply and Fan Status monitor displays two pie charts:

- Power Supply Units—On the node selected, shows the proportion of power supplies that are detected as absent against those that are present in the bay. Those units that are present indicate their operating status as OK, Check, or Failed. The totals shown below the title indicate the total number of power supplies that the device is capable of holding.
- Fans—On the node selected, shows the proportion of fans that are detected against those that are present in the bay. Those units that are present indicate their operating status as OK, Check, or Failed. The totals shown below the title indicate the total number of fans that the device is capable of holding.

Mouse over the pie segments to view the number of power supplies or fans in each segment. The total number of units is shown at the bottom of the graph. Click the details icon to open the Power Supply and Fan Status Details window.

Power Supply and Fan Status Details

The Power Supply and Fan Status Details window provides a tabular status view of each power supply and fan in the unit.

The top table lists all of the power supplies available in the device. Power supplies are listed by Flexible PIC Concentrator (FPC) and the numbered power supply associated

with the FPC. The chart shows the individual status of the power supply, such as OK, Absent, Check, or Failed.

The lower table lists the fans in the device. Fans are listed by Flexible PIC Concentrator (FPC) and the numbered fan associated with the FPC. The chart shows the individual status of the fan, such as OK, Absent, Check, or Failed.

Related Documentation

- Monitoring the Status of Standalone Switches on page 64
- Monitoring the Status of a Virtual Chassis on page 65
- Monitoring the Status of Virtual Chassis Members on page 66

QFabric Director Status Monitor

The Qfabric Director Status monitor shows the status of the QFabric director devices within the selected Directors folder in the View pane, in a table. It is on the Summary tab in Monitor mode. Table 41 on page 89 describes the table columns.

Table 41: Status Monitor for Qfabric Directors Table

Column	Description
Name	Device name.
Member ID	Member ID.
Status	Device status.
Role	Device role.
Uptime	Length of time the device has been up.

Related Documentation

- Understanding Monitor Mode in Network Director on page 3

QFabric Interconnect Status Summary Monitor

The QFabric Interconnect Status Summary monitor shows the status of the selected QFabric fabric's interconnect devices in a table. It is on the Summary tab in Monitor mode. Table 42 on page 89 describes the table columns.

Table 42: QFabric Interconnect Status Summary Monitor Table Description

Column	Description
Name	Device name.
Status	Device status.
Port Utilization %	Percentage of device's allocated bandwidth that is being used.

Table 42: QFabric Interconnect Status Summary Monitor Table Description *(continued)*

Column	Description
Uptime	Length of time the device has been up.

Related Documentation
- Understanding Monitor Mode in Network Director on page 3

QFabric VM Status Summary Monitor

QFabric VM Status Summary Monitor shows the status of the virtual machines (VMs) within the QFabric director device selected in the View pane, in a table. It is on the Summary tab in Monitor mode. Table 43 on page 90 describes the table columns.

Table 43: QFabric VM Status Summary Monitor Table

Column	Description
VM Name	Name of the VM.
CPU Utilization %	Percentage of CPU the VM is using.

Related Documentation
- Understanding Monitor Mode in Network Director on page 3

Radio Status Monitor

The Radio Status monitor, on the Equipment tab in Monitor mode, provides information about the radios and access points being controlled at this node. For example if you select Wireless Network, information about all of the radios is displayed; if you select a wireless controller, then only information for the radios for that controller is shown. The monitor has a summary view and a detailed view. The default view is the summary, showing four of the six available fields. These fields in the Radio Status monitor are described in Table 44 on page 90.

Table 44: Radio Status Monitor Fields

Field	Description	Summary, Detailed, or Hidden View
Radio Identifier	The system identification for the radio, composed of: • The access point name • A colon (:) • The radio number	Summary Detailed
MAC Address	The radio MAC address.	Summary (Hidden) Detailed

Table 44: Radio Status Monitor Fields *(continued)*

Field	Description	Summary, Detailed, or Hidden View
Status	Up (enabled), Down (disabled), or NA (unable to determine status).	Summary Detailed
Radio Type	The type of wireless clients that can connect to the access point.	Summary Detailed
Channel	The configured operating channel for AP communication.	Summary Detailed
Tx Power	The transmit power level for a radio.	Summary (Hidden) Detailed

Related Documentation

- Monitoring the Status of Aggregated Access Points and Radios on page 63
- Monitoring the Status of Wireless Controllers, Access Points, and Radios on page 67
- *Device Inventory Report*
- *Network Neighborhood Report*

Resource Utilization Monitor for Switches and Virtual Chassis

The Resource Utilization monitor shows a line chart for switch and Virtual Chassis CPU and memory use. The vertical axis shows the percentage of the resource being consumed. The horizontal axis shows the times when samples were taken. The time period that the chart represents is selectable from a list.

This monitor is available when you select either a standalone switch or a Virtual Chassis. It appears on the Equipment tab in Monitor mode.

This topic describes:

- Resource Utilization Summary on page 91
- Resource Utilization Details on page 92

Resource Utilization Summary

The summary view of the Resource Utilization monitor shows a line chart representing memory and CPU use. There are five categories shown on the chart:

CPU User—(Orange) the percentage of time that the CPU uses to run user processes, such as the database.

CPU System—(Green) the percentage of time that the CPU uses on all processes for the system.

CPU Background—(Light Blue) the percentage of time that the CPU uses on background processes.

CPU Interrupt —(Red) the percentage of time that the CPU uses for interrupt handling.

CPU Idle—(Purple) the percentage of time that the CPU is available for work.

5 min Mem avg—(Dark Blue) the amount of memory being used over a 5-minute average.

You can interact with the chart to manipulate the data being displayed by:

- Mouse the cursor over a line to highlight the line from the remaining items.
- Removing or restoring a line by clicking the legend item.
- Displaying specific chart values by mousing your cursor over the intersection of a vertical grid line and a data line.
- Changing the time period that the chart covers.

  If you select Custom, an additional dialog box opens, enabling you to select a starting and ending date and time.

Resource Utilization Details

In Resource Utilization Details, you can view utilization rates for memory and CPU over different periods of time. You can select the time period from a list or specify a custom value. If you select Custom, an additional dialog box, enabling you to select a starting and ending date and time.

The data is presented in two line charts or graphs, one for memory utilization and the other for CPU utilization. Select a time-frame for analysis from the list to update both graphs. Depending on the time-frame selected, the charts refresh to display time increments proportional to the time-frame. For example, if you select 1 Hour, the time increments are 5 minutes apart; if you select 1 day, the time increments are 1 hour apart. Mouse over the data intersections to view the precise value at that point.

Related Documentation

- Resource Monitor For Wireless LAN Controllers on page 92

Resource Monitor For Wireless LAN Controllers

The Resource Utilization monitor shows wireless LAN controller CPU and memory use for the last hour using two needle gauges. The gauges display usage from 1-100 percent as resources are consumed, making it easy to see if these resources are being under or overused.

This monitor is available when you select a wireless LAN controller. It appears on the Equipment tab when in Monitor mode.

This topic describes:

- Resource Utilization Summary on page 93
- CPU and Memory Utilization Charts on page 93

Resource Utilization Summary

The summary view of the Resource Utilization monitor displays two needle gauges:

- CPU Usage—For the selected node, it displays the device's CPU usage within the last hour marked in tenths from 0 to 100 percent. Under the gauge, the total percent usage is also shown.
- Memory Usage—For the selected node, it displays the device's memory consumption within the last hour marked in tenths from 0 to 100 percent. Under the gauge, the total percent usage is also shown.

To view the resource utilization over a period of 24 hours, a month, or a year, click the details icon. The CPU Utilization and Memory Utilization charts provide a more granular presentation of the data.

CPU and Memory Utilization Charts

The CPU and Memory Utilization charts allow you to view consumption rates for over different periods of time. You can select the time period from a list or specify a custom value. If you select Custom, an additional dialog box opens enabling you to select a starting and ending date and time.

The data is presented in two line charts or graphs, one for CPU utilization and the other for memory utilization. Select a time-frame for analysis from the list to update both graphs. Depending on the time-frame selected, the charts refresh to display time increments proportional to the time-frame. For example, when 1 Hour is selected, the time increments are 5 minutes apart; when 1 day is selected, the time increments are 1 hour apart. Mouse over the data intersections to view the precise value at that point.

Related Documentation

- Monitoring the Status of Wireless Controllers, Access Points, and Radios on page 67

RF Interference Sources Monitor For an Access Point

The RF Interference Sources monitor for single access points consists of a bar chart that reflects interference experienced with the traffic of one or both radios on the access point selected in the View pane. Some access points have two radios and some access points have one radio. Network Director tracks and monitors radio interference from these sources:

- Microwave ovens—Most domestic microwave ovens use 2.45 GHz, and can interfere with Wi-Fi channels from 8 to 10 (or even 7 to 11). Interference varies depending on the model of the oven—for example, commercial restaurant microwave ovens sweep over a wider spectrum and have a higher duty cycle.
- Continuous wave devices continuously transmit at a particular frequency without attempting to share the radio frequency medium with other devices. Devices that use continuous wave technology in the same frequency bands as wireless LAN networks will interfere with wireless communications, reducing performance or totally preventing

communication. Several examples of devices that may use continuous wave transmission that interferes with WiFi are video surveillance cameras and baby monitors.

- Bluetooth devices
- Phone FHSS from cordless phones
- Unknown devices

To track these interference devices, Network Director polls the access point's controller at the standard interval. The categories with the largest bars in the chart cause the most interference.

You can perform the following actions on the bar chart:

- Change the time period over which to display interference by selecting a time period from the list in the upper right corner.
- Display a numeric value by mousing over a bar in the chart.
- Add or remove one or both radio's data from the chart by clicking **Radio 1** or **Radio 2** in the legend.

Interference is frequently not a problem on wireless networks with light traffic, but as traffic becomes heavier, throughput and capacity decrease and other problems become apparent. RF interference can cause packet retransmission (see "Monitoring the Percentage of RF Packet Retransmissions" on page 48). Interference is also a security concern because jamming can bring down the network.

Ideally, interference retransmission does not cause more than 10% of the total number of packets sent. If your retransmission percentage is higher, you can try to lower it by:

- Locating and eliminating offending devices. If the item cannot be removed, you can add electromagnetic interference (EMI) shielding such as grounded mesh, foils, insulating foams, or insulating paint. This will limit the interference to a small area.
- Moving the affected access point.
- Moving clients to channels with less interference. Keep in mind, however, that Bluetooth devices, cordless phones, 802.11FH devices, and jamming emissions are broadband, so it's not possible to change channels away from them—they are everywhere in the band. For more information, see *Understanding Wireless Radio Channels* and *Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks*.

For more information about wireless interference, see "Understanding Wireless Interference" on page 54.

Related Documentation

- Monitoring RF Interference Sources For Radios on One Access Point on page 38
- Monitoring RF Interference Sources on Wireless Devices on page 41
- Monitoring RF Interference Sources on One Radio on page 38
- Understanding Wireless Interference on page 54
- *Understanding Wireless Radio Channels*

- *Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks*

RF Interference Sources Monitor for Wireless Devices

The RF Interference Sources monitor for wireless devices consists of a summary pie chart that reflects all wireless traffic experienced by the object selected in the View pane. You can select any one of the objects listed in Table 45 on page 95 in the view pane:

Table 45: Wireless Objects With Interference Tracking

Icon	Object
	Entire Wireless Network in any view.
	Wireless Mobility Domain in any view.
	Controller Cluster in any view. NOTE: You cannot see interference for a single controller.
	Individual access point in any view.
	Individual radio in any view.
	Selecting a floor in logical view displays all access points on that floor—to create a floor, see *Configuring Floors*.
	Selecting a building in logical view displays all access points in that building—to create a building, see *Configuring Buildings*.
	Selecting a site from the logical view displays all access points in that building—to create a site, see *Creating a Site*.
	Wiring closet—to create a wiring closet, see *Setting Up Closets*.

Network Director tracks and monitors interference from these sources:

- Microwave ovens—Most domestic microwave ovens use 2.45 GHz, and can interfere with Wi-Fi channels from 8 to 10 (or even 7 to 11). Interference varies depending on the model of the oven—for example, commercial restaurant microwave ovens sweep over a wider spectrum and have a higher duty cycle.
- Continuous wave devices continuously transmit at a particular frequency without attempting to share the radio frequency medium with other devices. Devices that use continuous wave technology in the same frequency bands as wireless LAN networks will interfere with wireless communications, reducing performance or totally preventing communication. Several examples of devices that may use continuous wave transmission that interferes with Wi-Fi are video surveillance cameras and baby monitors.

- Bluetooth devices
- Phone FHSS from cordless phones
- Unknown devices

To track these devices, Network Director polls the controllers at the standard interval. The categories with the largest sections of the pie chart cause the most interference.

You can perform the following actions on the pie chart:

- Change the time period over which to display interference by selecting a time period from the list in the upper right corner.
- Display a numeric value for interference occurrences by mousing over a section of the chart.
- Click the monitor's title to see a list of interfering objects along with the information listed in Table 46 on page 96.

Table 46: Information on RF Interference Sources for a Radio

Information	Description
Last Seen	Date and time the interference was last detected.
Transmitter ID	If the interference is caused by an object with a MAC address, the MAC address is displayed. If the object has no MAC address, MSS calculates a MAC address, using the characteristics of the object. This way, you can correlate interference events over time.
Listener MAC	MAC address of the access point that detected the interference.
AP	Name of the access point that detected the interference.
Controller	Name of the controller that reported the interference.
Channel	Channel the interference affected.
RSSI	Received signal strength indication (RSSI), in decibels referred to 1 milliwatt (dBm). A higher value indicates a stronger signal.
Duty Cycle	Reported fraction of time that the source is emitting RF.
Source Type	Possible sources of interference include Bluetooth, Continuous Wave, Microwave Oven, Unknown, and Phone FHSS.
CIM (%)	Estimated severity of interference on this channel caused by the source.

Interference is frequently not a problem on wireless networks with light traffic, but as traffic becomes heavier, throughput and capacity decrease and other problems become apparent. RF interference can cause packet retransmission (see "Monitoring the Percentage of RF Packet Retransmissions" on page 48). Interference is also a security concern because jamming can bring down the network .

Ideally, interference retransmission does not cause more than 10% of the total number of packets sent. If your retransmission percentage is higher, you can try to lower it by:

- Locating and eliminating offending devices. If the item cannot be removed, you can add electromagnetic interference (EMI) shielding such as grounded mesh, foils, insulating foams, or insulating paint. This will limit the interference to a small area.
- Moving clients to channels with less interference. Keep in mind, however, that Bluetooth devices, cordless phones, 802.11FH devices, and jamming emissions are broadband, so it's not possible to change channels away from them—they are everywhere in the band. For more information, see *Understanding Wireless Radio Channels* and *Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks*.

For more information about wireless interference, see "Understanding Wireless Interference" on page 54.

Related Documentation

- Monitoring RF Interference Sources on One Radio on page 38
- Monitoring RF Interference Sources For Radios on One Access Point on page 38
- Understanding Wireless Interference on page 54

RF Throughput Monitor

The Throughput monitor displays the amount of data throughput in kilobytes per second (KBps) experienced in the last hour by the object selected in the View pane. Total network throughput for each radio or for each access point (either one can be selected) is measured in KBps at the configured polling interval and plotted on this line chart. The throughput rates are reflected on the left side of the chart.

If you are viewing data for a time period longer than one hour, each data point on the graph represents data consolidated from more than one polling period. In this case, the graph shows multiple lines, which are labeled in the legend:

- maxThroughput—The largest value sampled during the consolidated polling periods.
- avgThrougput—The average of the values sampled during the consolidated polling periods.
- minThroughput—The smallest value sampled during the consolidated polling periods.

The area between the maxThroughput and minThroughput lines is shaded to indicate the range of values.

You can perform the following actions on this line graph:

- Change the time period over which to display throughput by selecting a time period from the list in the upper right corner.
- Display a numeric value by placing the cursor where a vertical grid line bisects a data line.

- Highlight a line in the graph by mousing over the line's legend.
- Remove or restore a line by clicking its legend.

Throughput data is available when you select either a radio or access point in any view of the View pane.

Throughput is decreased by Layer 2 retransmissions, increased numbers of clients, and the overhead associated with 802.11 protocols. You can try to increase throughput by:

- Adding equipment such as controllers and access points to cope with over-subscription.
- Using optimal configuration, such as WPA2 encryption, for 802.11n devices.
- Configuring separate WLAN Service profiles for voice and data—for data, see *Creating and Managing a WLAN Service Profile*. For directions on creating a voice-specific WLAN Service profile, see *Configuring a Voice SSID with Network Director* and *Creating a WLAN Service Profile Dedicated to Voice*.
- Creating separate Radio profiles for transmissions using long and short guard intervals—see *Creating and Managing a Radio Profile*.
- Locating and eliminating noise that could be causing interference. For more information, see "Monitoring RF Interference Sources on Wireless Devices" on page 41, "Monitoring RF Interference Sources on One Radio" on page 38, "Monitoring RF Interference Sources For Radios on One Access Point" on page 38, and "Monitoring RF Signal-to-Noise Ratio" on page 46.
- Checking for weak signals. If automatic power tuning is not enabled, try enabling it. For more information, see *Understanding Automatic Power Tuning for Wireless Radios*.
- Assigning access points to different channels. When channels are too congested, packet collision and corruption can occur. If automatic channel tuning is not enabled, try enabling it. For more information, see *Understanding Wireless Radio Channels* and *Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks*.
- Correcting conditions that trigger alarms - for a list of alarms, see the *Current Active Alarms Monitor*.

Related Documentation

- *Creating and Managing a WLAN Service Profile*
- *Configuring a Voice SSID with Network Director*
- *Creating a WLAN Service Profile Dedicated to Voice*
- *Creating and Managing a Radio Profile*
- Monitoring RF Interference Sources on Wireless Devices on page 41
- Monitoring RF Interference Sources on One Radio on page 38
- Monitoring RF Interference Sources For Radios on One Access Point on page 38
- Monitoring RF Signal-to-Noise Ratio on page 46
- *Understanding Automatic Power Tuning for Wireless Radios*
- *Understanding Wireless Radio Channels*

- *Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks*
- *Current Active Alarms Monitor*

Session Trends Monitor

The Session Trends monitor provides summary and detailed trend information about the number of active sessions within the node selected in the View pane.

NOTE: **After a device is discovered, trend data does not appear immediately—it appears only after three polling periods have occurred.**

Scope information: This monitor is available when you select the following nodes or node types in the View pane: The My Network node, switch, The Wireless Network node, wireless domain, wireless cluster, wireless controller, wireless access point, radio, site, building, or floor.

This topic describes:

- Session Trends on page 99
- Session Trends Details on page 100

Session Trends

The summary view of the Session Trends monitor displays a line graph of the number of active sessions over time within the node selected in the View pane. The vertical axis is the number of active sessions. The horizontal axis shows the polling interval times.

You can perform the following actions on the line graph:

- Change the time period over which to display the trend data by selecting a time period from the list in the upper right corner.
- Display the number of sessions at a polling interval by mousing over the intersection of the horizontal graph line and a vertical polling interval line.

If you are viewing data for a time period longer than one hour, each data point on the graph represents data consolidated from more than one polling period. In this case, the graph shows multiple lines, which are labeled in the legend:

- maxSessionCount—The largest value sampled during the consolidated polling periods.
- avgSessionCount—The average of the values sampled during the consolidated polling periods.
- minSessionCount—The smallest value sampled during the consolidated polling periods.

The area between the maxSessionCount and minSessionCount lines is shaded to indicate the range of values. You can perform the following actions using the graph legend:

- Highlight a line in the graph by mousing over the line's legend.

- Remove or restore a line by clicking its legend.

Session Trends Details

The Session Details window provides detailed trend information about the number of active sessions within the current node selected in the View pane. It contains these panes:

- The top pane contains a line graph of the number of active sessions over time within the node selected in the View pane.

  You can perform the following actions on the line graph:

  - Change the time period over which to display the trend data by selecting a time period from the list in the upper right corner.
  - Display the number of sessions at a polling interval by mousing over the intersection of the horizontal graph line and a vertical polling interval line.

  If you are viewing data for a time period longer than one hour, each data point on the graph represents data consolidated from more than one polling period. In this case, the graph shows multiple lines, which are labeled in the legend:

  - maxSessionCount—The largest value sampled during the consolidated polling periods.
  - avgSessionCount—The average of the values sampled during the consolidated polling periods.
  - minSessionCount—The smallest value sampled during the consolidated polling periods.

  The area between the maxSessionCount and minSessionCount lines is shaded to indicate the range of values. You can perform the following actions using the graph legend:

  - Highlight a line in the graph by mousing over the line's legend.
  - Remove or restore a line by clicking its legend.

- The bottom pane contains a table with detailed information about the active sessions.

The following table describes the columns that appear in current session details tables.

Table 47: Current Session Details Table

Table Column	Description
User Name	Client's user name
MAC Address	Client's MAC address.
Device Type	Client's device type.
Device Group	Client's device group.

Table 47: Current Session Details Table *(continued)*

Table Column	Description
Device Profile	Client's device profile.
Controller IP	IP address of the controller to which the client is connected.
AP ID	ID of the wireless access point to which the client is connected.
AP NAME	Name of the wireless access point to which the client is connected.
SSID	SSID to which a wireless client is connected.
VLAN	VLAN to which the client is connected.
Client IP	Client's IP address.
Auth Type	Authorization type used for the client.
B/w[KBps]	Bandwidth used by the client.
Node Name	Client's node name.
Data Usage (KBytes)	Data transmitted and received by the client, in kilobytes.
Elapsed Time	Length of time the session has been active.
Sample Time	Time when the most recent sample was taken.

TIP: Some table columns are hidden by default. To select which columns to display, mouse over any column heading, click the arrow that appears, mouse over **Columns** in drop-down menu, and then select the columns to display from the list.

Related Documentation

- Monitoring Client Sessions on page 29

Signal-to-Noise Ratio Monitor

- Monitoring Signal-to-Noise Ratio on page 101
- Signal-to-Noise Ratio Details on page 102

Monitoring Signal-to-Noise Ratio

Signal-to-noise ratio (SNR) is a measure of the level of a desired signal against the level of background noise, measured in decibels (dB). You can imagine this as a person trying to be heard in a noisy restaurant, where his voice is the signal and the background chatter

blocks his voice. The SNR charts display the ratio between signal and background noise, the individual signal level, and the individual background noise level.

If you are viewing data for a time period longer than one hour, each data point on the graph represents data consolidated from more than one polling period. In this case, the graph shows multiple lines, which are labeled in the legend:

- maxSnr—The largest value sampled during the consolidated polling periods.
- snr—The average of the values sampled during the consolidated polling periods.
- minSnr—The smallest value sampled during the consolidated polling periods.

The area between the maxSnr and minSnr lines is shaded to indicate the range of values.

You can perform the following actions on the SNR chart:

- Change the time period over which to display the SNR by selecting a time period from the list in the upper right corner.
- Display a numeric value by placing the cursor where a vertical grid line bisects a data line.
- Highlight a line in the graph by mousing over the line's legend.
- Remove or restore a line by clicking its legend.
- Click **Details** to view these three charts for a radio, one above the other:
  - Received signal strength indicator (RSSI), which measures the power of a radio signal
  - Signal to noise ratio (SNR) which measures a signal against the current RF background noise level
  - Noise floor which is the sum of all the noise interference for the radio—the current RF background noise level

Higher numbers on this chart indicate that a radio has more signal than noise, which is desirable. If the chart has more noise than signal (indicated by values less than 40 on the chart), the signal becomes more unreadable, because the noise level severely competes with it. A reading of 0-20 on this chart would indicate an unacceptable level of noise or a really low signal. This can cause a reduction in data speed because of frequent errors that require the source transmitter to resend data packets—see "Monitoring the Percentage of RF Packet Retransmissions" on page 48.

SNR is computed only for individual radios.

Signal-to-Noise Ratio Details

There are three charts in the Signal-to-Noise Ratio (SNR) Details window: RSSI, SNR, and Noise Floor. Table 48 on page 103 briefly describes how these charts can be interpreted.

Table 48: Interpreting Signal-to-Noise Ratio Values

	SNR	RSSI	Noise Floor
Definition	Signal-to-noise ratio is the ratio of a signal's strength to the sum of all interference. (Signal-to-noise Ratio = RSSI/Noise Floor).	RSSI is signal strength, the first value used in the signal-to-noise ratio.	Noise is any signal (interference) that is not Wi-Fi traffic such as cordless phones, microwaves, radar, etc. This is the second value in the signal-to-noise ratio.
How is it measured?	SNR is the ratio of signal to background noise, measured as a positive value between 0 dB and 80 dB. You want the signal to be high and the background noise to be low. This produces a higher ratio, which is better.	RSSI is measured in decibels from -20 through -100.	Noise floor is measured in decibels from -90 through -120.
What does the chart mean?	If the chart has more noise than a signal (indicated by values less than 40 on the chart), the signal becomes more unreadable, because the noise level severely competes with it. A reading of 0-20 on this chart would indicate an unacceptable level of noise.	A louder signal is better, so the higher the RSSI is, the better. Typically voice networks require a better signal level than a data network does. Normal signal strength in a network would be around -45 dB through -87 dB.	A quiet noise floor is better, so the closer to -120 the noise floor is, the better because that means there is little to no interference. Typical environment noise floors are about 95 dB.

Deal with a low SNR reading by either increasing the signal (RSSI) or reducing the background noise. To get an idea what an acceptable SNR reading is for your network, check the values when the network is operating optimally—you might be able to do this by changing the time period on the chart.

Related Documentation

- Monitoring RF Signal-to-Noise Ratio on page 46
- Monitoring the Percentage of RF Packet Retransmissions on page 48

Status Monitor for QFabric Directors

The Status monitor for QFabric Directors shows the status of the selected QFabric Director in a table. It is on the Summary tab in Monitor mode. Table 49 on page 103 describes the fields in this monitor.

Table 49: Status Monitor for QFabrics Directors Fields

Field	Function
Name	Device name.
Member ID	Member ID.
Status	Device status.
Uptime	Length of time device has been running.

Table 49: Status Monitor for QFabrics Directors Fields *(continued)*

Field	Function
Role	Device role.
IP Address	Device IP address.
VMs	Number of virtual machines (VMs) running on the device.

Related Documentation
- Understanding Monitor Mode in Network Director on page 3

Status Monitor for QFabric Interconnects

The Status monitor for QFabric Interconnects shows the status of the selected QFabric Interconnect in a table. It is on the Equipment tab in Monitor mode. Table 50 on page 104 describes the fields in this monitor.

Table 50: Status Monitor for QFabrics Interconnects Fields

Field	Function
Serial Number	Device serial number.
Model	Device model.
Status	Device status.
Uptime	Length of time device has been running.
Temperature	Device temperature, in degrees Celsius.

Related Documentation
- Understanding Monitor Mode in Network Director on page 3

Status Monitor for QFabric Nodes

The Status monitor for QFabric Nodes shows the status of the selected QFabric Node in a table. It is on the Equipment tab in Monitor mode. Table 51 on page 104 describes the fields in this monitor.

Table 51: Status Monitor for QFabrics Nodes Fields

Field	Function
Serial Number	Device serial number.
Model	Device model
Status	Device status.

Table 51: Status Monitor for QFabrics Nodes Fields *(continued)*

Field	Function
Uptime	Length of time device has been running.
Temperature	Device temperature, in degrees Celsius.

Related Documentation
- Understanding Monitor Mode in Network Director on page 3

Status Monitor for QFabrics

The Status monitor for QFabrics shows the status of the selected QFabric fabric in a table. It is on the Summary tab in Monitor mode. Table 52 on page 105 describes the fields in this monitor.

Table 52: Status Monitor for QFabrics Fields

Field	Function
Serial Number	Indicates the hardware serial number of the fabric.
IP Address	Indicates the IP address of the fabric.
Uptime	Indicates the amount of time since the last boot of the fabric in days, hours, minutes, and seconds.
Status	Indicates whether the fabric is up or down.
Used MAC Addresses	Indicates the number of MAC addresses in use on the fabric.
Used VLANs	Indicates the VLAN memberships for this fabric.
Last Configured Time	Indicates the date and time since the fabric was last configured.
Temperature Range (ºC)	Indicates the ambient temperature of the coldest and hottest devices in the fabric (in degrees Celsius).
Junos Version	Indicates the version and release level of Junos OS running on the fabric.

Related Documentation
- Understanding Monitor Mode in Network Director on page 3

Status Monitor for Switches

This monitor provides key information about the status for a standalone switch when a node is selected in any of the views. This monitor is on the Equipment tab in Monitor mode.

Table 53 on page 106 describes the fields in this monitor.

Table 53: Status Monitor Fields

Field	Function
Serial Number	Indicates the hardware serial number of the switch or Virtual Chassis.
IP Address	Indicates the IP address of the device.
Uptime	Indicates the amount of time since the last boot of the unit in days, hours, minutes, and seconds.
Status	Indicates whether the device is up or down.
Used MAC Addresses	Indicates the number of MAC addresses in use on the device.
Used VLANs	Indicates the VLAN memberships for this device.
Last Configured Time	Indicates the date and time since the device was last configured.
Temperature (ºC)	Indicates the ambient temperature (in degrees Celsius).
Junos Version	Indicates the version and release level of Junos OS running on the device.

Related Documentation

- Monitoring the Status of Standalone Switches on page 64

Status Monitor for Wireless Access Points

This monitor provides key information about the status for the wireless access point selected in any of the views. This monitor is on the Summary tab in Monitor mode.

Table 54 on page 106 describes the fields in this monitor.

Table 54: Status Monitor Fields

Field	Description
AP Name	Name of the access point.
AP Number	Number of the access point.
Model	The model number of the access point.
Serial Number	Serial number of the access point.
IP Address	The IP address assigned to the access point.
Uptime	The length of time since the access point last booted.

Table 54: Status Monitor Fields *(continued)*

Field	Description
status	Operational status of the access point: • Down—The access point is offline. • Up—The access point is online and enabled. • Up Redundant—The access point is online, reporting to this controller as redundant and another controller as primary.
Version	The version of the Mobility System Software (MSS) running on the access point.
Primary Controller	The primary controller for the access point.
Secondary Controller	The secondary controller for the access point.

Related Documentation
- Monitoring the Status of Wireless Controllers, Access Points, and Radios on page 67

Status Monitor for Virtual Chassis

This monitor provides status information, including power supply and fan information, for a Virtual Chassis. It is on the Equipment tab in Monitor mode.

The Summary view shows key status fields in a table format. Power supply and fan data is represented as small bar chart entries in the table. The Details view also shows the same status information, but expands the power supply and fan information. Table 55 on page 107 displays these fields and their location in the monitor.

Table 55: Virtual Chassis Status Monitor Fields

Field	Function	Location
Serial Number	Indicates the hardware serial number of the master member.	Summary Detailed
IP Address	Indicates the IP address of the master member.	Summary Detailed
Uptime	Indicates the amount of time since the last boot of the system in days, hours, minutes, and seconds.	Summary Detailed
Status	Indicates whether the Virtual Chassis is up or down.	Summary Detailed
Used MAC Addresses	Indicates the number of MAC addresses in use on the Virtual Chassis.	Summary Detailed
Used VLANs	Indicates the VLAN memberships for the Virtual Chassis.	Summary Detailed

Table 55: Virtual Chassis Status Monitor Fields *(continued)*

Field	Function	Location
Last Configured Time	Indicates the date and time since the Virtual Chassis was last configured.	Summary Detailed
Temperature Range (ºC)	Indicates the temperature of the coolest and hottest devices in the Virtual Chassis (in degrees Celsius).	Summary Detailed
Junos Version	Indicates the version and release level of Junos OS running on the device.	Summary Detailed
Power Supply Status	Indicates the number of power supplies that are detected as absent or present in the bay. The graphic bar and total count for missing and present power supplies is shown as OK, Check, or Failed.	Summary
Power Supply Status	In the Power Supply and Fan Status table, there are separate table entries for each power supply state with the totals for that state.	Detailed
Fan Status	Indicates the number of cooling fans that are detected as absent or present in the bay. The graphic bar and total count for missing and present fans is shown as OK, Check, or Failed.	Summary
Fan Status	In the Power Supply and Fan Status table, there are separate table entries for each power supply state with the totals for that state.	Detailed

Related Documentation

- Monitoring the Status of a Virtual Chassis on page 65
- Monitoring the Status of Virtual Chassis Members on page 66

Status Monitor for Virtual Chassis Members

Use the Member Status monitor to view key information about the status of Virtual Chassis members. It is displayed on the Equipment tab in Monitor mode when you select a Virtual Chassis member.

Table 56 on page 108, describes the fields in this monitor.

Table 56: Status Monitor for Members Fields

Field	Description
Serial Number	Indicates the hardware serial number of the member.
Member ID	Identifies by number a member switch in a Virtual Chassis.
Member Serial Number	Indicates the hardware serial number of the member.
FPC Slot	Identifies the Flexible PIC Concentrator (FPC) slot number for the member: same as Member Slot.

Table 56: Status Monitor for Members Fields *(continued)*

Field	Description
Member Model	The model number of the member.
Member Mixed Mode	Indicates whether the switch is configured to run in mixed member mode. Valid fields are true or false.
Member Role	Indicates the function and responsibility of the switch in the Virtual Chassis. Possible values are master, backup, and linecard.

Related Documentation

- Monitoring the Status of Virtual Chassis Members on page 66

Status Monitor for Wireless LAN Controllers

The Status monitor for wireless LAN controllers provides status highlights for the wireless controller. View Table 57 on page 109 for a description of the fields in the monitor.

This monitor is available on the Equipment tab when you select a wireless controller from any view while in Monitor mode.

Table 57: Wireless Controller Status Fields

Field	Function
Serial Number	Indicates the hardware serial number of the master member.
IP Address	Indicates the IP address of the master member.
Uptime	Indicates the amount of time since the last boot of the system in days, hours, minutes, and seconds.
Status	Indicates whether the controller is up or down.
MSS Version	Indicates the version and release level of Mobility System Software running on the device.

Related Documentation

- Monitoring the Status of Wireless Controllers, Access Points, and Radios on page 67

Top Sessions by MAC Address Monitor

The Top Sessions by MAC Address monitor provides summary and detailed information about the sessions within the node you selected in the View pane that use the most bandwidth. This monitor is available in the Client tab.

This monitor includes only wireless network sessions, not sessions on wired connections. If the node you selected in the View pane contains only wired sessions, this monitor does not appear. If the node contains both wired and wireless sessions, only the wireless sessions appear in the monitor.

This topic describes:

Top Sessions

The summary view of the Top Sessions by MAC Address monitor displays a bar chart of the sessions within the node you selected in the View pane that consume the most bandwidth. The vertical axis shows the session MAC addresses. The horizontal axis shows different information depending on the time period you select in the list in the title bar:

- If you select the **Current** time period, the horizontal axis shows the session's incremental data usage.
- If you select any time period other than **Current**, the horizontal axis shows the session's total data usage.

You can mouse over a bar to see more information about that session.

Top Session by MAC Details

The Top Session by MAC Details window displays detailed information about the top sessions within the node you selected in the View pane.

To change the number of top sessions displayed, select a number from the Top *N* list in the upper right corner.

To change the time period for which data is shown, select a time period from the time period list. By default, the Current time period is selected. When Current is selected, the data from the most recent polling period is shown. When any time period other than Current is selected, the data for the entire selected time period is shown.

The following table describes the columns that appear in Top Sessions by MAC Details table.

Table 58: Top Session Details Table

Table Column	Description
User Name	Client's user name To copy the text in this table cell: Click the cell, highlight the text, right-click the cell, and select **Copy** from the context menu.
MAC Address	Client's MAC address. To copy the text in this table cell: Click the cell, highlight the text, right-click the cell, and select **Copy** from the context menu.
Number of Sessions	Number of sessions.
AP Name	Name of the wireless access point to which the client is connected.

Table 58: Top Session Details Table *(continued)*

Table Column	Description
AP ID	ID of the wireless access point client is connected to.
Incremental Data Usage (KBytes)	The session's current incremental data usage. Appears only when the Current time period is selected.
Total Data Usage (KBytes)	The session's total data usage. Appears when any time period other than Current is selected.

Related Documentation

- Monitoring Client Sessions on page 29

Top Users Monitor

The Top Users monitor provides summary and detailed information about the users within the node you selected in the View pane that use the most bandwidth. This monitor is available on the Client tab.

This monitor includes only wireless network users, not users on wired connections. If the node you select in the View pane contains only wired users, this monitor does not appear. If the node contains both wired and wireless users, only the wireless users appear in the monitor.

This topic describes:

- Top Users on page 111
- Top Session By User Details on page 111

Top Users

The summary view of the Top Users monitor displays a bar chart of the top bandwidth users within the node you selected in the View pane. The vertical axis shows the user names. The horizontal axis shows different information depending on the time period you select in the list in the title bar:

- If you select the **Current** time period, the horizontal axis shows the user's incremental data usage.
- If you select any time period other than **Current**, the horizontal axis shows the user's total data usage.

You can mouse over a bar to see more information about that user.

Top Session By User Details

The Top Session By User Details window displays detailed information about the top users within the node you selected in the View pane.

To change the number of top users displayed, select a number from the Top *N* list in the upper right corner.

To change the time period for which data is shown, select a time period from the time period list. By default, the Current time period is selected. When Current is selected, the data from the most recent polling period is shown. When any time period other than Current is selected, the data for the entire selected time period is shown.

The following table describes the columns that appear in Top Session By Users Details table.

Table 59: Top Session Details Table

Table Column	Description
User Name	Client's user name To copy the text in this table cell: Click the cell, highlight the text, right-click the cell, and select **Copy** from the context menu.
MAC Address	Client's MAC address. To copy the text in this table cell: Click the cell, highlight the text, right-click the cell, and select **Copy** from the context menu.
Number of Sessions	Number of sessions.
AP Name	Name of the wireless access point to which the client is connected.
AP ID	ID of the wireless access point client is connected to.
Incremental Data Usage (KBytes)	The session's current incremental data usage. Appears only when the Current time period is selected.
Total Data Usage (KBytes)	The session's total data usage. Appears when any time period other than Current is selected.

Related Documentation

- Monitoring Client Sessions on page 29

Traffic Trend Monitor

The Traffic Trend monitor displays inbound and outbound traffic trends on the node you selected in the View pane. This monitor is available in the Traffic tab. A line graph shows the rate of each type of traffic over time. The horizontal axis shows the times when samples were taken. The vertical axis shows the data rate, in packets per second.

NOTE: After a device is discovered, trend data does not appear immediately—it appears only after three polling periods have elapsed.

You can perform the following actions on the line graph:

- Change the time period over which to display the traffic trends by selecting a time period from the list in the upper right corner.
- Highlight a line in the graph by mousing over the line's legend.
- Remove or restore a line by clicking its legend.
- Display a numeric value by mousing over where a vertical grid line crosses a data line.

Related Documentation

- Monitoring Traffic on Devices on page 21

Unicast vs Broadcast/Multicast Monitor

The Unicast vs Broadcast/Multicast monitor displays a pie chart of the current distribution of unicast, broadcast, and multicast traffic types on the node you selected in the View pane. This monitor is available in the Traffic tab.

The traffic is divided into these categories:

- Unicast inbound
- Unicast outbound
- Broadcast inbound
- Broadcast outbound
- Multicast inbound
- Multicast outbound

Mouse over a pie segment to view the actual number of packets.

Related Documentation

- Monitoring Traffic on Devices on page 21

Unicast vs Broadcast/Multicast Trend Monitor

The Unicast vs Broadcast/Multicast Trend monitor displays trends in the data rates of unicast, broadcast, and multicast traffic on the node you selected in the View pane. This monitor is available on the Traffic tab. A line graph shows the rate of each type of traffic over time. The horizontal axis shows the times when samples were taken. The vertical axis shows the data rate, in packets per second.

NOTE: **After a device is discovered, trend data does not appear immediately—it appears only after three polling periods have elapsed.**

The traffic is divided into these categories:

- Unicast inbound
- Unicast outbound
- Broadcast inbound
- Broadcast outbound
- Multicast inbound
- Multicast outbound

You can perform the following actions on the line graph:

- Change the time period over which to display the traffic trends by selecting a time period from the list in the upper right corner.
- Highlight a line in the graph by mousing over the line's legend.
- Remove or restore a line by clicking its legend.
- Display a numeric value by mousing over where a vertical grid line crosses a data line.

Related Documentation

- Monitoring Traffic on Devices on page 21

Virtual Chassis Topology Monitor

The Virtual Chassis Topology monitor provides a fast and simple way to view the members and their relationships. It is available on the Equipment tab in Monitor mode. View Table 60 on page 114 for a description of the fields in the monitor.

The summary shows up to five available fields that you can configure to be displayed or hidden. The details page shows an expanded version with up to eleven fields that can also be tailored.

Table 60: Virtual Chassis Topology Fields

Field	Function	Default in Topology Monitor
Member	Identifies by member ID a member switch in a Virtual Chassis.	Summary (hidden) Details (hidden)
Member Role	Indicates the function and responsibility of the switch in the Virtual Chassis. Possible values are master, backup, and linecard.	Summary Details
Member ID	Same as Member.	Summary Details

Table 60: Virtual Chassis Topology Fields *(continued)*

Field	Function	Default in Topology Monitor
FPC Slot	Identifies the Flexible PIC Concentrator (FPC) slot number for the member.	Summary Details
Member Status	Identifies whether the member is present in the Virtual Chassis or Not Present.	Details
Member Serial Number	Identifies the hardware serial number of the switch.	Details
Member Model	Specifies the Juniper model number of the switch.	Details
Member Location	Identifies the wiring closet for the switch.	Details (hidden)
Member Mixed Mode	Indicates whether the switch is configured to run in mixed member mode. Valid fields are true or false.	Details
Neighbor ID	Identifies the neighbors by the member ID.	Summary Details
Neighbor Interface	The Virtual Chassis Port of the neighbor.	Details

Related Documentation

- Monitoring the Status of a Virtual Chassis on page 65