

HP OpenView Enterprise Discovery

for the Windows[®] operating system

Software Version: 2.20

Migrating from Network Discovery

Manufacturing Part Number: None
Document Release Date: April 2007
Software Release Date: April 2007



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

© Copyright 1993-2007 Hewlett-Packard Development Company, L.P.

Trademark Notices

Microsoft®, Windows®, Windows NT®, and Windows® XP are U.S. registered trademarks of Microsoft Corporation.

Windows Vista™ is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Java™ is a US trademark of Sun Microsystems, Inc.

UNIX® is a registered trademark of The Open Group.

Support

You can visit the HP Software Support web site at:

<http://support.openview.hp.com/support.jsp>

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To find more information about access levels, go to:

http://support.openview.hp.com/new_access_levels.jsp

Contents

1	Introduction	7
	Why Read This Guide?	7
	The Complete Set of Enterprise Discovery Licenses	7
	License Options	8
	Automated Inventory	8
	Hardware Requirements for the Alarms License	8
2	Enterprise Discovery Alarms	9
	Line Breaks	9
	Utilization	9
	Delay	11
	Jitter	11
	Collisions	11
	Broadcasts	11
	Errors	12
	Frame Relay	12
	Device Breaks	12
	Packet Loss	12
	Disk Utilization	13
	CPU Utilization	13
	Load Average	13
	Memory Utilization	13
	Backplane Utilization	13
	Printer	13
	UPS	13
	Port MTTR	13
	Port MTBF	14
	Port Moves	14
	Device MTTR	14
	Device MTBF	14
	Device Moves	14
	Alarms and Events	15
	Aggregate Health and Events	16
	Table Reading and Polling	16
3	Network Data Analysis + Alarms	17
	Health Panel, Alarms Viewer, and Network Map	18
	Service Analyzer	19
	Full-Path Graphs	21
	Events Browser	22

Reports	23
Report statistics	23
Executive/Summary Network Reports	24
WAN Reports.....	28
LAN Reports	30
Device Reports	31
Device Manager	33
State.....	33
Statistics	33
Port Manager	36
State.....	36
Statistics	36
Line Manager.....	37
State.....	37
Attribute Manager.....	37
Statistics	37
4 Changing Alarm Thresholds	39
Device Types.....	39
Line Alarm Types.....	40
Copying alarm thresholds	41
5 Other Benefits of the Alarms License	43
Enhanced Notification Data in SNMP Traps	43
Additional Event Filter Criteria	44
Index.....	53

1 Introduction

Why Read This Guide?



Read this guide only if you are upgrading from Peregrine's Network Discovery software.

If you were using Network Discovery, and have migrated to the new Enterprise Discovery 2.20, you have a license that is not available to all Enterprise Discovery users. This “Alarms license” provides you with extra alarm data that was available with Network Discovery. This way, you can migrate to the new versions of Enterprise Discovery without losing any of the functionality you are accustomed to having.

As you read through the normal set of Enterprise Discovery documentation, you will notice that several alarms and related features are not discussed at all. These alarms are only available for you and will be covered in this document.

Most of the functionality is the same with or without the Alarms license, but there are several subtle differences throughout the User Interface.

The Complete Set of Enterprise Discovery Licenses

In order to keep these features separate from the rest of Enterprise Discovery, they are packaged with an Alarms license. The following packages are available, with Alarms being included in options 6, 7, and 8:

Table 1 License Options^a

Option	Contents
1	Automated Inventory
2	Automated Inventory + Software Utilization
3	Automated Inventory + Network Topology
7	Automated Inventory + Network Topology + <i>Alarms</i>
4	Automated Inventory + Network Topology + Software Utilization
8	Automated Inventory + Network Topology + Software Utilization + <i>Alarms</i>

- a. The Discovery + Network Topology license combination is also available to customers who upgrade from previous versions of Enterprise Discovery. The Discovery license provides basic information on the devices, such as when they are added to or removed from the network.

License Options

Automated Inventory

With this license, Enterprise Discovery will ping and poll your network device groups to find devices. You can also create scanners to scan your network servers and workstations. You can automatically deploy agents to these devices, and then deploy the scanners to determine the hardware and software installed on each device. This data is combined with the Discovery data in the Enterprise Discovery database.



The Automated Inventory license provides the same capability that the Device Discovery and Device Inventory licenses provided in previous versions of Enterprise Discovery. If you have purchased these two licenses for a previous version, you will have access to all features provided with the Automated Inventory license offered with version 2.20.

Software Utilization

With this license, you can expand your inventory data, as the scanners will capture details on what software is used on each Windows workstation, and report how often it is used and who is using it. You will see this Utilization data appear in the Scan Data Viewer, and in Reports.

Network Topology

With this license, you can expand your discovery data by calculating and displaying connectivity information for your network. Adding a topology license means that you will find additional alarms in the Health Panel/Alarms Viewer. This also adds many new Reports.

Alarms

The Alarms option was designed specifically for users of Peregrine Network Discovery who need to upgrade to Enterprise Discovery. The standard Enterprise Discovery package does not include these extra alarms and attributes. This option will give you more alarms in the Health Panel, in reports, and more attribute information throughout the web UI (for example, Service Analyzer, Device Manager, or Port Manager).

Hardware Requirements for the Alarms License

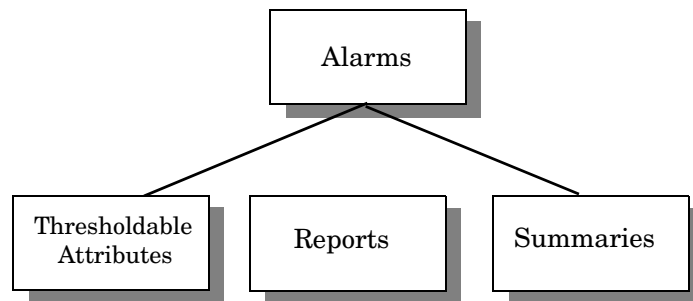
The features available to you with the Alarms license do not require additional memory, processor speed, or disk space. The hardware requirements listed for the Topology license in the *HP OpenView Enterprise Discovery Installation & Initial Setup Guide* are sufficient for the Alarms license as well.

2 Enterprise Discovery Alarms

The Alarms license gives you access to a large number of statistics and attributes. An attribute is the type of data being monitored, such as Utilization or Delay. When the value of that attribute crosses a specific threshold, it will cause an alarm in Enterprise Discovery, and that alarm will be reflected in the Health Panel and the Alarms Viewer. An alarm can have 4 different values: info, minor, major, or critical.

Events can be caused by a change in an attribute's alarm state (for example, an attribute going from OK to Major would be considered an event). Events can also be caused by other scenarios, such as adding a new device, or changing a device property such as its icon or title. All of these events will be reflected in the Events Browser.

The following diagram shows the Enterprise Discovery Alarm hierarchy.



Thresholdable Attributes can cause alarms (critical, major, minor, info). These are thresholds that the user can change. These events are reflected in the Health Panel the next time a value is collected for that attribute (the database is refreshed once per minute). To see what attributes can be “alarmed” see the “Can be Thresholded” column in the table at **Help > Classifications > Supported Device/Port Attributes**. To change the thresholds, from the Network Map or Health Panel, click **Edit > Alarm Thresholds**.

The following sections describe the types of alarms you will be able to see in the Health Panel and elsewhere in the web UI.

Line Breaks

Identifies lines that are broken. A line is broken when its status is down and the line break is not due to devices at either end being broken.

Utilization

Identifies lines that are used heavily—that is, that have a lot of traffic. Describes the amount of traffic on the line as a percentage of capacity.

Available only to devices with byte counters or frame counters. For media with variable length packets, utilization is calculated by directly reading bytes counts from every interface. For media with fixed length packets (for example, ATM cells), utilization is derived from frame counts.

On the Port Manager Statistics panel, you will see three Utilization graphs:

- Utilization In
- Utilization Out
- Line Utilization

Utilization In and Out

In and Out utilization for Half Duplex and Full Duplex ports are calculated using a common algorithm.

In both cases, Enterprise Discovery reads the byte/frame count and port speed for each interface from the device MIB. Enterprise Discovery calculates the bit count per second by computing the difference between two successive byte/frame counts and dividing this by the poll period. The port utilization is calculated by dividing the bit count per second by the port speed.

For variable: In Utilization is calculated by taking the InByte count per port, converting this value to the Bit per second value, dividing by the Port speed, and multiplying by 100 to get a percentage. i.e. $[(\text{InByte} \times 8\text{Bits}) / \text{Port Speed}] \times 100$.

For fixed length: In Utilization is calculated by taking the InFrame count per port, converting this value to the Bit per second value, multiplied by the number of bytes per frame, dividing by the Port speed, and multiplying by 100 to get a percentage. i.e. $[(\text{InFrame} \times 8\text{Bits} \times \text{BytesperFrame}) / \text{Port Speed}] \times 100$.

Out Utilization is similarly calculated by taking the OutByte (or OutFrame) count per port.

Line Utilization

Line utilization is determined using different methods, depending on whether the ports are Half Duplex or Full Duplex.

Half Duplex

Line Utilization is equal to the total of InUtilization and OutUtilization. Unlike Full Duplex, the IN and OUT on a Half Duplex line occur on the same channel, and the value for one limits the value of the other. Given a 100 Mbps Half Duplex line, if the IN traffic is 90 Mbps, the OUT traffic can be at most 10 Mbps. In all cases, the sum of both values cannot exceed 100 Mbps. As a result, it makes sense to use the sum of the IN and OUT to calculate the line utilization. If this total reaches a threshold, an alarm is triggered.

Full Duplex

Line Utilization for a full duplex port is the maximum value of either the In or Out Utilization.

Enterprise Discovery calculates line utilization this way because the primary objective is to inform the user whenever the line utilization becomes a concern. It becomes a concern whenever it approaches the maximum utilization (or reaches a threshold and triggers an alarm). For a Full Duplex line, the In and Out occur on two separate channels, and the value for one does not limit the value of the other. The values are independent of each other, and

their values are limited only by the line speed. Given a 100 Mbps Full Duplex line, for example, the In traffic may be 90 Mbps while the Out traffic may be 30 Mbps, but each cannot exceed 100 Mbps.

Delay

Delay is calculated for lines, however the delay values are associated with the ports at both ends of the line. The delay values for the two ports will be the same.



It is possible to alarm only one end of the line if the interface types (and alarm thresholds) are different.

Delay alarms identify lines with long queuing delays. The response time, measured in milliseconds, is a portion of the time taken by a device to respond to a ping. This includes the following:

- the time a packet waits in the router queue before being transmitted
- the time to process the packet at the other end after being received



The calculation does not include the delay across the link.

The values are calculated based on round trip delays (ping responses) from the devices at both ends of the line. The round trip delay for a device is the mean of the ping responses received during a poll cycle.

The delay value is half the difference between the mean round trip delays of the two devices minus the lowest value recorded for this line.



Enterprise Discovery receives one ping per poll cycle for the scheduled request and will receive some additional pings for fast break requests.

Jitter

Jitter is calculated as the difference between the delay value for the current poll cycle and the delay value for the previous poll cycle. It is measured in milliseconds, and is bi-directional.



Jitter does not appear in the Health Panel, but it does appear in the Service Analyzer “summary graphs” panel, and in the State panel of the Device Manager.

Collisions

Identifies the number of collisions per second detected on every line in the network with values above the thresholds.

Broadcasts

Identifies the number of broadcasts per second detected on every line in the network with values above the thresholds. Broadcasts are part of normal network operation, but large numbers of broadcasts must be investigated and the cause rectified.

There are three types of broadcast alarms:

- Broadcast In

- Broadcast Out
- Source of Broadcast

Source of Broadcast alarms only occur in devices that Network Discovery has determined to be broadcast sources such as servers, routers and workstations.

Broadcast In and Broadcast Out can apply to any device showing high broadcast levels, including switches and FDDI devices which are not seen as a sources of broadcasts, but as devices that forward the broadcast sent to them. Only source of broadcast alarms are seen in the event log.



When you are looking for the source of a broadcast, set the priority on your map window to 1. This will help you determine which workstation might be causing the broadcasts.

Errors

Identifies the number of errors per second detected on every line in the network with values above the thresholds.

Exactly what errors are reported depends on the MIBs of the devices at either end of the line. Not all devices detect all errors.

Frame Relay

Attributes relating to your frame relay connections: Data Delivery Ratio, Frame Delivery Ratio, Discard Eligibility In, Discard Eligibility Out, BECN, FECN.

Device Breaks

Identifies when a device is no longer accessible by Enterprise Discovery.

Packet Loss

Identifies managed core network devices (for example, routers and switches) that are dropping frames. Describes the percentage of frames that are dropped by each managed device. Calculated on unicast data, inbound and outbound, for all ports of the device. Percentage is calculated over the past 5 sampling periods.

The criteria for Enterprise Discovery to calculate “Packet Loss” is as follows:

- The device must be router or a switch.
- All ports of the device must have unicast counter attributes.
- All ports must have valid port statistics (i.e. if a port does not have a valid counter, such as if the statistics filtered out by the mapping module for any reason, the “Packet Loss” attribute will not be calculated).
- If a port has status bit up but has frames and unicast counters “0”, the “Packet Loss” attribute will not be calculated. Even if it has out statistics different than “0”.



If a port has in or out frames 0 but in or out unicast = 0, the “Packet Loss” attribute will not be calculated.

Packet loss is calculated on a per device basis, more specifically if there are backplane connections to your devices the packet loss statistics might be slightly “off”.

Disk Utilization

The percentage used on each disk partition.

CPU Utilization

The percentage of the cycles used by each processor.

Load Average

A calculation of how much of the CPU is being used.

Example: If the CPU is all being used, it's maxed out for scheduled processes, then the load average will be 1. If there are twice as many processes scheduled than the CPU can handle, the load average will be 2.

Memory Utilization

The memory used by all running processes.

Backplane Utilization

For some Cisco devices, taken from a MIB variable.

Printer

Paper count.

UPS

UPS battery capacity and UPS battery time remaining.

Port MTTR

Mean time to repair (MTTR) identifies ports that take a long time to repair. A running average of the number of hours broken against how many times it was broken.

Example: A port has failed twice. The first time, it was broken for 4 hours. The second time, it was broken for 8 hours. The MTTR for this device is $(4 + 8) / 2 = 6$ hours.

Port MTBF

Mean time between failures identifies ports that fail frequently. A running average of the number of days in operation measured against the number of times a ports has failed.

Example: A port has been in operation for 100 days and Enterprise Discovery has seen it fail twice. The MTBF for this device is 50 days.

Port Moves

Identifies if the connection to a device has changed from one port to another.

Example: A workstation is attached to a switch at port 2. You detach the workstation from port 2, and reattach it to port 8. That would create a Port Move event. The change is recorded on the workstation, not the switch. The workstation has not necessarily changed location, only the switch port to which it connects.

Device MTTR

Mean time to repair (MTTR) identifies devices that take a long time to repair. A running average of the number of hours broken against how many times it was broken.

Example: A device has failed twice. The first time, it was broken for 4 hours. The second time, it was broken for 8 hours. The MTTR for this device is $(4 + 8) / 2 = 6$ hours.

Device MTBF

Mean time between failures identifies devices that fail frequently. A running average of the number of days in operation measured against the number of times a device has failed.

Example: A device has been in operation for 100 days and Enterprise Discovery has seen it fail twice. The MTBF for this device is 50 days.

Device Moves

Identifies devices recently moved, or had a change in connection to the network.

Moves are not reported for devices that have been added recently. If a device appears in Adds, it will not appear in Moves.

The time to detect changes in connectivity depends on the sampling period for the network.

Example: A workstation is attached to a switch. You detach the workstation, and reattach it to another switch. That would create a Device Move event, because Network Discovery thinks the workstation has changed location. The change is recorded on the workstation, not the switch. The workstation has not necessarily changed location, only the switch to which it connects.

Notes

- Does not include connector devices as anchor devices—connections to a connector device are not considered relevant
- Does not include cases where the current and previous connections are to connector devices

- Does not include cases where the current and previous connections are the same, or are probably the same (as in the cases where the only one connection is known).

Alarms and Events

➤ When reading this explanation, assume that the server can record data for 100,000 ports, and a total of 20 attribute for each port. That means each Enterprise Discovery server can record a total of 2,000,000 attributes.

Each attribute recorded by Enterprise Discovery can have thresholds associated with it. The thresholds relate to alarm types: OK, Info, Minor, Major, Critical. An event is triggered each time an attribute changes state (for example, from OK to Minor, or Minor to OK). An alarm is created if the attribute state value is within an alarm threshold (Info, Minor, Major, Critical).

For example, you could set your Disk Space thresholds to the following settings:

- OK - 0-10%
- Info - 10-20%
- Minor - 20-40%
- Major - 40-75%
- Critical - 75-100%

If the value of the event falls within an alarm range (for example, Disk space is 90% full), an alarm will be created (in this example, a Critical alarm).

Once Enterprise Discovery creates an alarm, this triggers a message to the internal “event notification system.” If the user has created an Event Filter (**Administration > Event Filter Configuration**) for this change of alarm state, the user will be notified immediately through an e-mail, pager message, or SNMP trap.

➤ When you are creating Event Filters, you can input a notification delay. This means that Enterprise Discovery will not notify you of the alarm until after the delay period, in case the problem is quickly corrected.

All new values are cached to show the current state of the device. Once a minute (see Note below), that state is updated in the Enterprise Discovery internal database. Every 30 seconds, the Health Panel checks the database for updates and refreshes the user interface. The user can press the F5 key to request an immediate database query. The refresh time should be less than 1 sec.

➤ How often the states are updated in the database depends on how many attributes you are monitoring. If you have <500,000, the database is updated every minute. If you have 1,000,000 attributes, the database is updated every two minutes.

The Health Panel also shows reporting data:

- Add/Delete/Move/Change/Exceptions are updated in the database every 15 minutes (it could be longer with large networks).
- MTTR/MTBF are updated once per day
- Not Recently Seen

Aggregate Health and Events

The Aggregate Health Panel works a bit differently. There are a few more steps involved.

First, it relies on the above being completed on each server. The Health Panel data is then extracted from the realtime database and made available to the aggregator. Like the regular Health Panel, this also has a time delay depending on the number of attributes in the database. If you have <500,000 attributes, the database is updated every 5 minutes. For each additional 100,000 attributes, the database takes an additional minute to update (for example, if you have 700,000 attributes, the database will update every 7 minutes).

Once the data is imported into the Reports database, the data is then available for aggregation (the Reports database is visible via ODBC).

Every 5 minutes, the aggregator server will check if there is any data available on each of the configured remote servers. If so it will transfer the data and put it in an incoming queue.

Also every 5 minutes the aggregator checks the incoming queue for each server configured to see if there are any files waiting. If so they are processed. If there a lot of files to process from many servers, the time waiting in the queue will increase.

In a situation where the aggregator is not overloaded, and the network is not slow in transferring the file from the remote server to the aggregator server, you should see your data within 15 minutes.

Table Reading and Polling

Table reading and polling produce the majority of network traffic from the Enterprise Discovery server. These functions provide:

- connectivity information
- discovery of devices (for example, MAC-only devices)
- collection of statistics
- break fault analysis

A poll is really one frame out and one frame back in most cases. The number of polls for a device will depend on the number of ports in the device, and the number of attributes collected for each port (for example, collisions, broadcasts, etc.). The device itself is also pinged in each poll cycle.

Consider the fact that collecting statistics on a router with 200 ports requires a lot more effort than collecting statistics from a workstation with one port.

3 Network Data Analysis + Alarms

With the addition of the Alarms license to your Enterprise Discovery server, you will see more data throughout the web user interface. See the total list of available alarms in [Chapter 2, Enterprise Discovery Alarms](#).

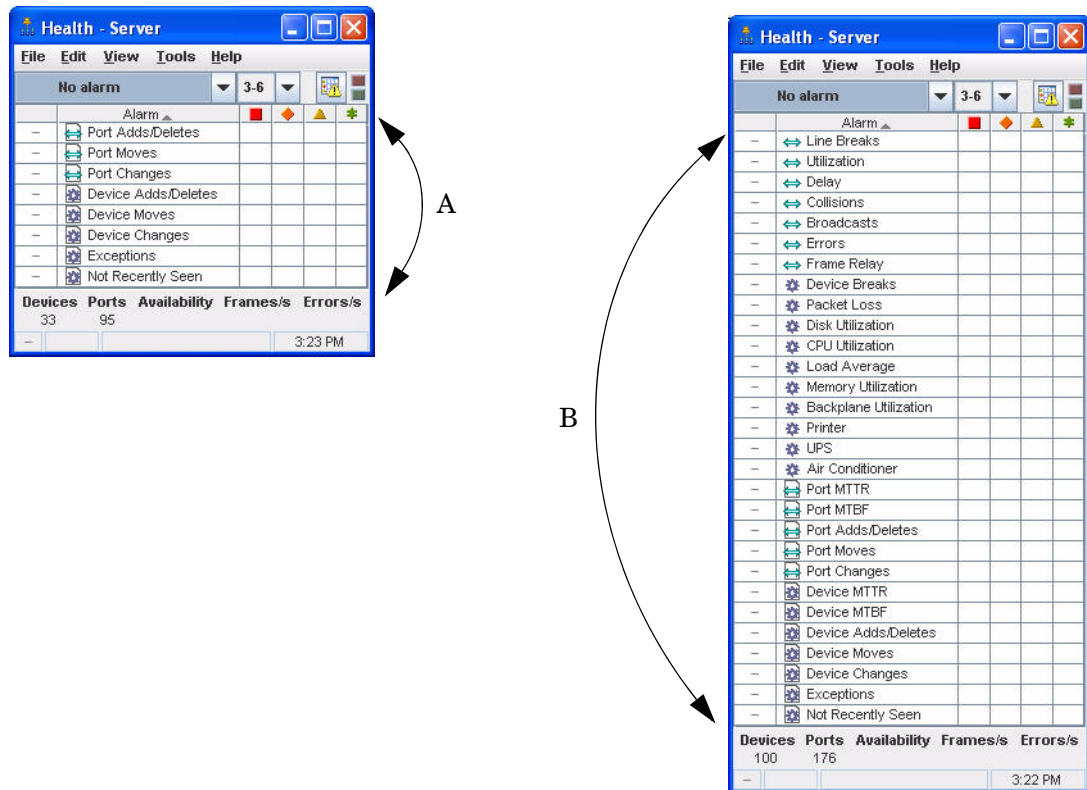
The *Network Data Analysis Guide* provides detailed information on the features that deal with the device data discovered through network polling. These features will all have small differences if you have an Alarms license:

- [Health Panel, Alarms Viewer, and Network Map](#) on page 18
- [Service Analyzer](#) on page 19
- [Events Browser](#) on page 22
- [Reports](#) on page 23
- [Device Manager](#) on page 33
- [Port Manager](#) on page 36
- [Line Manager](#) on page 37
- [Attribute Manager](#) on page 37

Health Panel, Alarms Viewer, and Network Map

The Health Panel displays all the Alarm categories available on your Enterprise Discovery server. To see the whole list available to you, click **View** and deselect **Hide Inactive Alarms**.

In the following diagram, you can see the additional alarm categories displayed with the Alarms license (B).



The Alarms Viewer and Network Map look the same regardless of your license, with only the available alarms appearing.

Service Analyzer

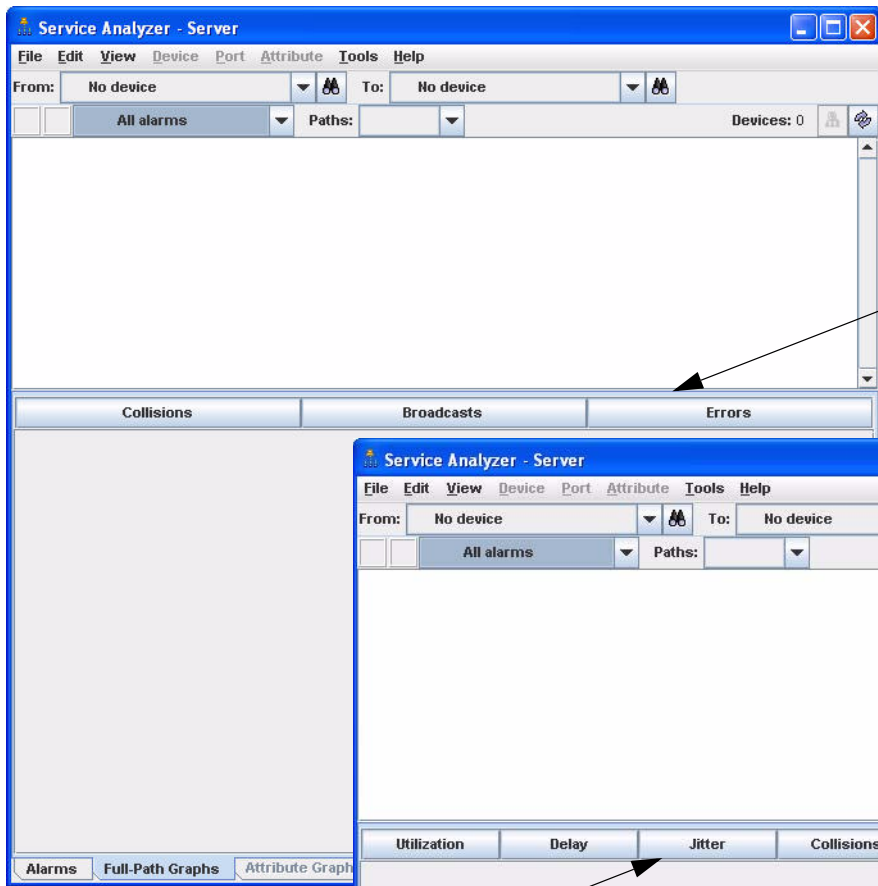
The Service Analyzer has very few changes with the addition of the Alarms license.

Without the Alarms license, you will see the following alarm categories on the Full-Path Graphs tab (A):

- Collisions
- Broadcasts
- Errors

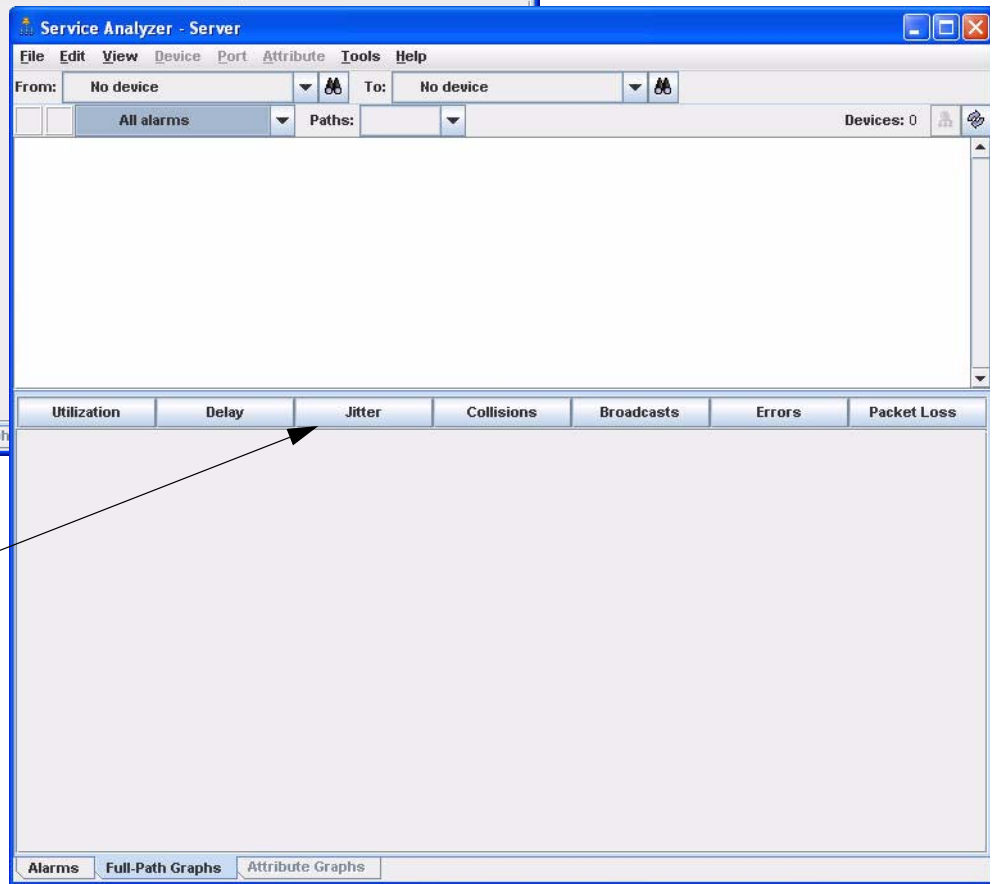
With the Alarms license, you will see the following alarm categories on the Full-Path Graphs tab (B):

- Utilization
- Delay
- Jitter
- Collisions
- Broadcasts
- Errors
- Packet Loss



A

B



Full-Path Graphs

The Full-Path Graphs tab shows a summary of the entire path for the following alarm categories:

Table 2 Graphs

Alarm Category	Notes
Utilization	Utilization in percentage; for ports, bi-directional
Delay	Delay in milliseconds; for ports
Jitter	Jitter (change in delay) in milliseconds; for ports, bi-directional
Collisions	Collisions per seconds; for ports
Broadcasts	Broadcasts in frames/sec.; for ports, bi-directional
Errors	Errors in frames/sec.; for ports
Packet Loss	Packet loss in percentage; for devices

Events Browser

The Events Browser displays all recent events (Network or User Access events) on your network. With the Alarms license, you will see more alarms listed here (B), similar to what appears in the other features of the web user interface.

A

Device	Port	Attribute	Value
172.22.1.36	416	Device Changes: Default Title	172.22.1.36 (ws9200-1.ottawa.loran.com)
2.22.1.36	416	Port Changes: Port 416	Ethernet 100 FD (Ethernet 100 HD)
2.22.1.36	416	Port Changes: Port 416	Full Duplex (Half Duplex)
2.22.1.36	415	Port Changes: Port 415	Ethernet 100 FD (Ethernet 100 HD)
2.22.1.36	415	Port Changes: Port 415	Full Duplex (Half Duplex)
2.22.1.36	413	Port Changes: Port 413	Ethernet 100 FD (Ethernet 100 HD)
2.22.1.36	413	Port Changes: Port 413	Full Duplex (Half Duplex)
2.22.1.36	412	Port Changes: Port 412	Ethernet 100 FD (Ethernet 100 HD)
2.22.1.36	412	Port Changes: Port 412	Full Duplex (Half Duplex)

B

Device	Port	Attribute	Value
SKIDROW		Device Changes: Default Title	SKIDROW (172.22.6.235)
SKIDROW		Device Changes: Default Tag	ED 2.1 (IP Only Device)
SKIDROW		Device Changes: Default Priority	3 (1)
SKIDROW		Device Changes: Default Icon	Discovery Server (Unknown)
SKIDROW	1.4	Port Adds: Port 1.4	
2.22.5.3		Device Changes: Default Title	172.22.5.3 (webcreature.reboot.loran.com)
2.22.1.36		Device Changes: Default Title	172.22.1.36 (ws9200-1.ottawa.loran.com)
2.22.1.36		Device Changes: Default Tag	WaveSwitch 9200 (IP Only Device)
2.22.1.36		Device Changes: Default Priority	4 (1)
2.22.1.36		Device Changes: Default Icon	Enterprise Switch Layer 2 or below (Unknown)
2.22.1.36	516	Port Adds: Port 516	
2.22.1.36	515	Port Adds: Port 515	
2.22.1.36	514	Port Adds: Port 514	
2.22.1.36	513	Port Adds: Port 513	
2.22.1.36	512	Port Adds: Port 512	
2.22.1.36	511	Port Adds: Port 511	
2.22.1.36	510	Port Adds: Port 510	
2.22.1.36	509	Port Adds: Port 509	
2.22.1.36	508	Port Adds: Port 508	
2.22.1.36	507	Port Adds: Port 507	

Reports

Reports are also dependent on license. If you have the Alarms license (B), you will see reports about alarms, performance issues, and resource-managed devices.

Executive/Summary Network Reports Network Documentation Inventories of local devices in the network by various classifications and in several formats	
Scanned Device Reports Scanned Device Summaries Summary counts of locally scanned devices grouped by different device properties with drill-down to device details Applications Local software application license and installation counts grouped by application, version, and publisher Unrecognized Files Summary and detail reports of unrecognized application files found on scanned devices.	
WAN Reports Frame Relay Frame Relay inventory reports Point to Point Serial Point to Point Serial line inventory report Serial to Service Provider Network Service Provider Network Serial line inventory report Digital Subscriber Line (DSL) Digital Subscriber line inventory report ATM ATM line inventory report WAN Wide WAN Wide line inventory report	
LAN Reports LAN Backbone LAN Backbone line inventory report FDDI FDDI line inventory report Token Ring Token Ring inventory report	
Device Reports Servers Servers inventory report Routers Routers inventory report Input and Output Devices I/O Devices inventory report Web Servers Web Servers inventory reports	

A

Executive/Summary Network Reports Network Documentation Inventories of local devices in the network by various classifications and in several formats Performance Summaries Graphical summaries of network performance as a whole and various subsets of the network Alarm Summaries Devices and ports alarmed during the report period Network Wide Network wide device availability, line utilization and throughput	
Scanned Device Reports Scanned Device Summaries Summary counts of locally scanned devices grouped by different device properties with drill-down to device details Applications Local software application license and installation counts grouped by application, version, and publisher Unrecognized Files Summary and detail reports of unrecognized application files found on scanned devices.	
WAN Reports Frame Relay Summary and detailed Frame Relay reports Point to Point Serial Summary and detailed Point to Point Serial line reports Serial to Service Provider Network Summary and detailed Service Provider Network Serial line reports Digital Subscriber Line (DSL) Summary and detailed Digital Subscriber line reports ATM Summary and detailed ATM line reports WAN Wide Summary and detailed WAN Wide line reports	
LAN Reports LAN Backbone Summary and detailed LAN Backbone line reports FDDI Summary and detailed FDDI line reports Token Ring Summary and detailed Token Ring line reports	
Device Reports Servers Inventory, availability, and resource summaries for Servers, resource utilization details for resource managed Servers Routers Inventory, availability, and resource summaries for Routers, resource utilization details for resource managed Routers Input and Output Devices Inventory, availability, and resource summaries for I/O devices, resource utilization details for resource managed I/O devices, and paper usage reports Resource Managed Workstations Inventory, availability, and resource summaries for Resource Managed Workstations, resource utilization details Web Servers Inventory, availability, and resource summaries for Web Servers, resource utilization details for resource managed Web Servers	

B

The following section explains all the Reports available with an Alarms License. To see the other reports available, see the *Network Data Analysis Guide*.

Report statistics

Many reports feature bar graphs and values for three statistics: the peak, the mean peak, and the mean.

A mean value and a peak value are collected for every sample. At the end of the report period, all peak values are used to calculate the mean peak.

Imagine that we record a mean value and a peak value three times a day:

Table 3 Statistics Example

Value	first	second	third
Mean	2.0	2.0	3.0
Peak	6.0	7.0	6.0

To obtain the mean peak for the day, we take the peak values of 6.0, 7.0, and 6.0, and find the mean of those three values, which is 6.3.

Different report periods have different statistical sampling periods. For example, a report with the period “Yesterday” takes samples every five minutes.

Executive/Summary Network Reports

Executive Summary reports are about the network as a whole. Here is one example of how you might use them—just to see what’s in your network.

To view the Executive/Summary Network Inventory Reports

- Click **Reports > Network Documentation > Device Inventory Summary**
- Or click **Reports > Network Documentation > Device Inventory**

You may have very little idea of what is actually in your network beyond the core network devices:

- There may be several people responsible for the network.
- Someone or several people may be adding equipment without informing you.
- You may be new to the job and the last person didn’t keep complete records or records you can understand.
- Some or all of the network management may have been delegated to someone outside your organization.
- You may be outside the organization whose network you must manage.

The Device Inventory Summary report tells you what is in your network, and the Device Inventory report tells you in more detail.

The following Reports are available:

Folder	Report	Type
Network Documentation	Network Classification	pie graph, table
	Network Devices by Function	pie graph, table
	End Nodes by Function	pie graph, table
	Device Inventory Summary	table
	Device Inventory by Category	table
	Device Inventory by UNSPSC	pie graph, table
	Device Inventory by Virtual LAN	table
	Port Inventory by Virtual LAN	table
	Device Inventory	list
	Resource Managed Device Inventory	list
	Device Resource Inventory	list
	Resource Managed Device Attributes	list
	Resource Inventory and Usage	table
	Frame Relay PVC Inventory	table
	Possible Modems Report	list
	Underutilized Equipment	table
	End Node Top Talkers	table
	End Node Top Listeners	table

Folder	Report	Type
Performance Summaries	Network Summary Reports	line/bar graphs
	WAN Summary Reports	line/bar graphs
	Frame Relay Summary Reports	line/bar graphs
	Serial to SPN Summary Reports	line/bar graphs
	DSL Summary Reports	line/bar graphs
	Point to Point Summary Reports	line/bar graphs
	ATM Summary Reports	line/bar graphs
	LAN Backbone Summary Reports	line/bar graphs
	FDDI Summary Reports	line/bar graphs
	Token Ring Summary Reports	line/bar graphs

Folder	Report	Type
Alarm Summaries ^a	Line Breaks	table
	Line Utilization ^a .	table
	Delay	table
	Collisions	table
	Broadcasts	table
	Errors	table
	Frame Relay FDR/DDR	table
	Frame Relay FECN/BECN	table
	Discard Eligibility In/Out	
	Device Breaks	
	Packet Loss	
	CPU Utilization	
	Memory Utilization	
	Load Average	
	Disk Utilization	
	Virtual Memory Utilization	
	Backplane Utilization	
	Paper Count	
	UPS Battery Capacity	
	UPS Battery Time Remaining	
Network Wide	Network Availability	line/bar graphs
	Mean Network Utilization ^b	line/bar graphs
	Peak Network Utilization ^c	line/bar graphs
	Mean Network Throughput ^b .	line/bar graphs
	Peak Network Throughput ^c .	line/bar graphs
	Inventory	list
	Availability Details	table
	Utilization Details	table

- a. Line alarm reports include connected lines only.
- b. For the Mean graphs, only mean values are used, so the lines represent the “mean of the means.”
- c. For the peak graphs, only peak values are used. This means that the bars on the graphs represent the highest peak utilization value of all the peak values from the network devices.

Performance Summaries

These folders contain the following periods:

- Today
- Last 7 Days
- Last Week
- This Month
- Last Month

Alarm Summaries

These folders contain the following periods:

- Yesterday
- Last 7 Days
- Last Week
- This Month
- Last Month

Network Wide

The folders for Availability Details and Utilization Details contain the following periods:

- Yesterday
- Last 7 Days
- Last Week
- This Month
- Last Month

WAN Reports

Frame Relay reports, as an example, can tell you if you are getting the service you are paying for. Note, for instance, the Data Delivery Ratio Report, one of the detailed reports. The Data Delivery Ratio Report tells you which Permanent Virtual Circuits (PVCs) are dropping data and is a good guide to whether or not you are getting the Frame Relay service you are paying for and whether you could do with less.

To view a Data Delivery Ratio Report:

- Click **Reports > WAN Reports > Frame Relay Service > Data Delivery Ratio**

There are two report structures for WAN Reports:

- Frame Relay folder
- all other folders

Frame Relay Summary Reports

Frame Relay Availability

Frame Relay Mean Utilization

Frame Relay Peak Utilization

Frame Relay Mean Throughput

Frame Relay Peak Throughput

Frame Relay Detail Reports

Inventory

Connected DLCI Inventory

Availability Details

Mean Time Between Service Outage (MTBSO)

Mean Time To Service Repair (MTTSR)

PVC Utilization

Over Utilized PVCs

Under Utilized PVCs

Interface/DLCI Utilization

Congested PVCs

Data Delivery Ratio (DDR)

Frame Delivery Ratio (FDR)

Unconnected Frame Relay Ports

Delay Details

In the following table, <WAN_type> stands for one of the following:

- Point to Point (Serial)
- Serial to SPN (Service Provider Network)
- DSL (Digital Subscriber Line)
- ATM (Asynchronous Transfer Mode)
- WAN (WAN Wide)

Report/Folder	Type
Summary Reports	
<WAN_type> Availability	line/bar graphs
Mean <WAN_type> Utilization	line/bar graphs
Peak <WAN_type> Utilization	line/bar graphs
Mean <WAN_type> Throughput	line/bar graphs
Peak <WAN_type> Throughput	line/bar graphs
Detail Reports	
Inventory	list
Availability Details	table
Utilization Details	table

LAN Reports

LAN reports give you inventory information and information about the availability, throughput and utilization of your Local Area Network whether you have a LAN backbone, FDDI, or Token Ring.

In the following table, <LAN_type> stands for one of the following:

- LAN Backbone
- FDDI
- Token Ring

Report/Folder	Type
Summary Reports	
<LAN_type> Availability	line/bar graphs
Mean <LAN_type> Utilization	line/bar graphs
Peak <LAN_type> Utilization	line/bar graphs
Mean <LAN_type> Throughput	line/bar graphs
Peak <LAN_type> Throughput	line/bar graphs
Detail Reports	

Report/Folder	Type
Inventory	table
Availability Details	table
Utilization Details	table

The folders for Availability Details and Utilization Details contain the following periods:

- Yesterday
- Last 7 Days
- Last Week
- This Month
- Last Month

Device Reports

Device reports give you inventory information and information about availability, throughput and utilization, broken down by category of device. They can also give you such information as what servers are using the most memory for a given time.



The Inventory report exported to a CSV file reflects the default map configuration for the current account.

All other reports reflect the Prime map configuration and its packaging.

Device reports are available for the following groupings of devices:

- Servers
- Routers
- Input and Output Devices
- Resource Managed Workstations
- Web Servers

Report/Folder	Type
All Devices	
Inventory	list
Availability Details	table
Utilization Details	table
Resource Managed	
Top CPU Utilization	table
Top Memory Utilization	table

Report/Folder	Type
Top Load Average	table
Disk Utilization Greater than 50%	table
Virtual Memory Utilization Greater than 5%	table

The Resource Managed folders contain the following:

- Inventory
- Yesterday
- Last 7 Days
- Last Week
- This Month
- Last Month



The Web Servers reports will reflect the default map configuration for the current account.

Device Manager

The following buttons will be available in the Device Manager only if you have an Alarms license.

	State	This panel displays current values for attributes. For more information, see page 33 .
	Statistics	This panel provides a second toolbar with which to view or export detailed historical statistics of the device. The statistics may be viewed in graph or table form, and may be exported in Comma Separated Value (CSV) form. For more information, see page 33 .

State

This panel displays current values for attributes.

This panel is not available if the object is not in the Enterprise Discovery database.

Attributes

See **Help > Classifications > Supported device/port attributes**.

The displayed attributes will differ depending on whether or not the device is managed, the type of device, and if resource management is configured.

- The Enterprise Discovery server itself will have the most attributes because you will see attributes for the server, and for the network as a whole.
- The Enterprise Discovery server itself will not have any Breaks or Total Breaks data.

Information on attributes is collected from the network regularly (during each poll cycle). The information is the latest available, and so may be different each time you view it. Enterprise Discovery only shows you attributes that are relevant.

When data in a table has a gray background, the data shown is considered stale, because it was obtained before the beginning of your selected time period.

A blank space indicates that data is not available for a device or port.

- If a device had a partitioned disk, each partition will appear as a separate “Disk” attribute. You can open an Attribute Manager for each partition. Each partition may have a different disk serial number (assigned by the device OS).

Statistics

This panel provides a second toolbar with which to view or export detailed historical statistics of the device. The statistics may be viewed in graph or table form, and may be exported in Comma Separated Value (CSV) form.

Not all statistics are available for all devices. Only available statistics appear in the list box. Statistics are a subset of Attributes ([Attributes](#) on page 33).

Statistics for the past two to three days are averaged every five minutes, statistics for the past 33 days are averaged every hour, and statistics for the past 365 days are averaged every day.



The y-axis maximum pull-down list only applies when graphing data. It allows you to change the topmost data point on the y-axis. Some of the options may have no effect on the display depending on the actual data. The highest data point is always shown, regardless of your selection.

Graph

Whenever a graph contains multiple averages, the data is adjusted to the lowest common denominator and the data points used are indicated on the graph. For example, a graph of the past seven days contains only one-hour data points.

At the beginning of data collection, Enterprise Discovery shows whatever data it has at five-minute intervals—even if you want to see statistics for long periods of time. This can be changed if you select a different option from the granularity pull-down list.

Gray portions of the graph indicate that data was not available for a period. Darker gray is used for unavailable data plotted in dark blue, lighter gray for unavailable data plotted in light blue. Also shown on the graph are horizontal lines representing alarm thresholds (depending on the option you have selected in the pull-down list).

You can change the graph by changing the selection in any of the pull-down lists. You can change the statistic, the interval, the maximum levels, and the granularity of data displayed.



Every account can have its own default settings for the statistic, interval, maximum levels, and granularity. See **Administration > Account administration > Account properties**.

Table

The table shows a tabular view of the statistics.

Export

Creates a Comma Separated Value (CSV) file of the data. Popular spreadsheets such as Microsoft Excel can import CSV files if you want to sort or graph the statistics in a way that is beyond the capabilities of Enterprise Discovery.

Statistics

Available statistics depend on the device model.

Notes on some statistics:

- **Total Breaks:** This statistic reports cumulative values.
- **Downtime:** This statistic reports cumulative values.
- **Total In Bytes:** Some devices do not report traffic in bytes, so this menu item may not appear. For such devices, try **Total In Frames**.
- **Total Errors:** Includes only errors in that the device stores in its MIB. Enterprise Discovery does not control which errors are stored, and cannot report errors that the device does not chose to store.
- **Total Collisions:** Only available for Ethernet half duplex. Also restricted to devices that report collisions in the dot3StatsEntry object of their MIB.

Interval

Past 2 hours | Past 4 hours | Past 6 hours | Past 12 hours | Past 24 hours | Past 48 hours | Past 7 days | Past 30 days | Past 90 days | Past 180 days | Past 365 days | Today | This week | This month | This quarter | This half | This year | Last week | Last month | Last quarter | Last half | Last year

Maximum

These attributes show the Max value of the vertical axis. If you have set alarm thresholds (Utilization, Delay, etc.), the Threshold Max is shown with a red line.

Selection	Description
Threshold Max	The vertical axis will show the maximum threshold value, if the thresholds have been configured.
Data Max	The vertical axis will show the maximum value of the data gathered.
Data Max with Thresholds	Same as “Data Max.” However, if thresholds have been configured, they will be displayed as horizontal lines.
Attribute Max	Used for graphs such as Utilization, Availability, or Disk Space so that the Vertical axis is adjusted according to the Max value of these Attributes. For example, the maximum level for Utilization is 100%.
Attribute Max with Thresholds	Same as “Attribute Max.” However, if thresholds have been configured, they will be displayed as horizontal lines.





The y-axis maximum drop down list only applies when graphing data. It allows you to change the topmost data point on the y-axis. Some of the options may have no effect on the display depending on the actual data. The highest data point is always shown, regardless of your selection.

Granularity

Default granularity | 5-minute granularity | Hourly granularity | Daily granularity

Port Manager

The following panels are available in the Port Manager only if you have an Alarms license or a Topology license. A subset of the State and Statistics information is available without the Alarms license, but if you have the Alarms license, more information is displayed.

Icon	Button name	Description
	State	This panel displays current values for attributes. For more information, see page 36 .
	Statistics	This panel provides a second toolbar with which to view or export detailed historical statistics for the port. The statistics may be viewed in graph or table form, and may be exported in Comma Separated Value (CSV) form. For more information, see page 36 .

State

This panel displays current values for attributes.

This panel is not available if the object is not in the Enterprise Discovery database.

Table

There is a list of supported device and port attributes in **Help > Classifications > Supported Device/Port Attributes**.

These values are collected from the network regularly and may change each time they are viewed. The values shown are the latest information available.

When data in a table has a gray background, the data shown is considered stale, because it was obtained before the beginning of your selected time period. To change the time before data is considered stale, see the section on Account Properties in the *Configuration and Customization Guide*.

The left-most column is for attributes that are associated with the alarm categories on the Health Panel. The alarm icon in this column tells you at a glance if the port is experiencing problems. The column also includes Operational Status.

A blank space indicates that data is not available for a device or port.

Statistics

This panel provides a second toolbar with which to view or export detailed historical statistics for the port. The statistics may be viewed in graph or table form, and may be exported in Comma Separated Value (CSV) form.

Inbound and outbound data is displayed for several statistics. Average values and peak values are available for several statistics.

Not all statistics are available for all ports. Only available statistics appear in the list box. Statistics are a subset of Attributes (see Help > Classifications > Supported Device/Port Attributes).

The Statistics panel in the Port Manager works the same as in the Device Manager. See the description above in [Device Manager](#) on page 33.

Line Manager

The following column in the Line Manager About panel is available only if you have an Alarms license.

State

In the About panel, the left-most column for each device tells you at a glance if either device or the port of either device is experiencing any problems for any attribute. Unlike in map windows, the Line Manager displays alarm signals even when the priority for the device (and its ports) is less than the minimum priority for a configuration. A blank space indicates that data is not available for a device or port.

Attribute Manager

The following button will be available in the Attribute Manager only if you have an Alarms license.

Statistics

This panel provides a second toolbar with which to view or export detailed historical statistics for the attribute. The statistics may be viewed in graph or table form, and may be exported in Comma Separated Value (CSV) form.



“No data available” means that no data has yet been collected for the attribute. This is normal if the device or port was discovered less than 48 hours before.

The Statistics panel in the Attribute Manager works the same as in the Device Manager. See the description in [Statistics](#) on page 33 in [Device Manager](#).

4 Changing Alarm Thresholds

Enterprise Discovery generates alarms of different severity depending on where you set the thresholds.

The Alarm Thresholds feature lets you set alarm levels for all the functions that Enterprise Discovery monitors. Any changes to the Alarm Thresholds apply globally to all accounts.



If you have an Alarms license, you can view alarm threshold settings regardless of the type of Enterprise Discovery logon account that you have. To set or modify attribute thresholds, however, you must have either an IT Manager account or an Administrator account.

You can access the Alarm Thresholds menu from any map window. Click **Edit > Alarm Thresholds**. You can check all your alarm thresholds at **Status > Current Settings > Device alarm thresholds/Line alarm thresholds**.

There are a few important notes you should know before you change alarm thresholds:

- One alarm value can be associated with multiple ranges. For example, you can apply a Critical alarm range if your line utilization is too high or too low.
- You do not need to cover the entire range of possible values. You can only create thresholds for the levels that you care about
- You can clean alarms with the “Alarm State Timeout” in **Administration > System Configuration > Network devices**.

Device Types

Enterprise Discovery initially sets all thresholds to default values. If a value of a threshold has not been set for a device type, the default will be used.

Alarm Thresholds - MD Demo

Threshold Selection

Attribute: ⚙️ Packet Loss

Line alarm type:

Device type: 🔌 Switch Layer 3 or above

Threshold Values

☒ Default ☐ Custom

Low	High	State
10	25	▲
25	+	◆

Units: %

Add Remove

Copy Paste

Apply OK Cancel

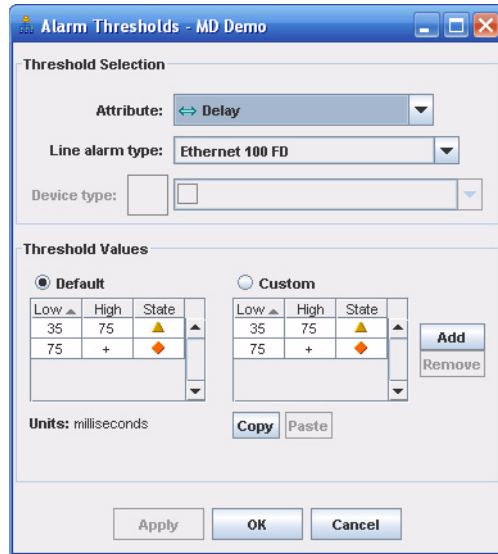
To change the Device Alarm Thresholds

- 1 Select a device attribute from the pull-down list.
The **Device type** list is enabled.
- 2 Select a device type by clicking an icon from the pull-down list.
- 3 To change an alarm threshold, click a text box and enter a new number for the low or high value.
- 4 To create a new alarm threshold, click the **Add** button and a new row will appear.
- 5 To change the State of any alarm, click the box in the State column, and select the new state from the list that appears.
- 6 Click **Apply** or **OK**.

If the values for different states overlap, a warning message will appear, and the affected values will be highlighted in red.

Line Alarm Types

Enterprise Discovery initially sets all threshold values to default values. If a value of a threshold has not been set for a line type, the default will be used.



To change the Line Alarm Thresholds

- 1 Select a line attribute from the pull-down list.
The **Line alarm type** list is enabled.
- 2 Select a line alarm type from the pull-down list.
- 3 To change an alarm threshold, click a text box and enter a new number for the low or high value.
- 4 To create a new alarm threshold, click the **Add** button and a new row will appear.
- 5 To change the State of any alarm, click the box in the State column, and select the new state from the list that appears.
- 6 Click **Apply** or **OK**.

If the values for different states overlap, a warning message will appear, and the affected values will be highlighted in red.

Copying alarm thresholds

If you wish to use the same alarm threshold values for different device or line types, you can use the **Copy** and **Paste** buttons.

To copy alarm thresholds

- 1 Select the custom alarm threshold setting you want to duplicate.
- 2 Click **Copy**.
- 3 Select an attribute from the pull-down list.
- 4 Select a line or device type from the pull-down list.
- 5 Click **Paste**.

The alarm thresholds you selected in step 1 will now appear in the custom area of the Alarm Thresholds dialog for the newly selected attribute and device/line alarm type.

- 6 Click **Apply** to apply the changes.
- 7 Click **OK** to close the dialog.

5 Other Benefits of the Alarms License

Enhanced Notification Data in SNMP Traps

When the Alarms license is installed, the following additional information is included in the notification when Enterprise Discovery issues a trap using SNMPv2c messages:

Table 1 deviceEvent Notification Information

Order	Object	Type	Description
5	state .1.3.6.1.4.1.11.2.17.18.0.1.2.4	Integer	Alarm state of the event: info (Add, Delete, PropertyChange, ConnectionChange), na-ok, na-info, na-minor, na-major, na-critical, ok-na, ok-info, ok-minor, ok-major, ok-critical, info-na, info-ok, info-minor, info-major, info-critical, minor-na, minor-ok, minor-info, minor-major, minor-critical, major-na, major-ok, major-info, major-minor, major-critical, critical-na, critical-ok, critical-info, critical-minor, critical-major.
14	value .1.3.6.1.4.1.11.2.17.18.0.1.2.8	Octet String	Value of threshold variable that triggered event. Value is not present where it makes no sense, for e.g. categories break, add, or delete.
15	units .1.3.6.1.4.1.11.2.17.18.0.1.2.9	Integer	The unit of the Value. Units always appear whenever Value does. Can be one of: notAvailable, count, day, persec, percent, hour, unknown.

Table 2 portEvent Notification Information

Order	Object	Type	Description
5	state .1.3.6.1.4.1.11.2.17.18.0.1.2.4	Integer	Alarm state of the event: info (Add, Delete, PropertyChange, ConnectionChange), na-ok, na-info, na-minor, na-major, na-critical, ok-na, ok-info, ok-minor, ok-major, ok-critical, info-na, info-ok, info-minor, info-major, info-critical, minor-na, minor-ok, minor-info, minor-major, minor-critical, major-na, major-ok, major-info, major-minor, major-critical, critical-na, critical-ok, critical-info, critical-minor, critical-major.
20	alarmType .1.3.6.1.4.1.11.2.17.18.0.1.2.6.8	Unsigned 32	The alarm type for this port.
22	value .1.3.6.1.4.1.11.2.17.18.0.1.2.8	Octet String	Value of threshold variable that triggered event. Value is not present where it makes no sense, for e.g. categories break, add, or delete.
23	units .1.3.6.1.4.1.11.2.17.18.0.1.2.9	Integer	The unit of the Value. Units always appear whenever Value does. Can be one of: notAvailable, count, day, persec, percent, hour, unknown.

Additional Event Filter Criteria

You can send pager and email messages whenever a device attribute changes state. In addition to the basic filter criteria described in Chapter 4, “Setting Up Event Filters,” in the *Configuration and Customization Guide*, you can specify a state transition for a particular attribute group.

The following three examples demonstrate how you can use alarm thresholds to design an event filter.

Examples of common Event Filters

There are many ways to set up event filters. Sometimes, it is difficult to understand all the possible implications.

It is always best to create simple and specific event filters that are easy to understand.

Read this section to understand how to create a few common, simple, and helpful event filters. If you have more questions, please call Customer Support.

Example 1: Notification when a core device breaks

A core device can be any important device in your network. For example, you may consider a particular type of ATM Switch to be very important, and you may want to know when that device is broken. For this example, we will set up an event filter that will page an Administrator account when this type of ATM Switch goes down.

Before you start the procedure, make sure the following has all been done properly:

- Your pager equipment has been installed and configured.
- Your pager service provider information is correct and up to date.

To set up the Administrator account:

- 1 Click **Administration > Account administration > Account contact data**.
- 2 Select the Administrator account that you want to change.
- 3 Click **Modify Properties**.
- 4 Enter the correct pager information:
 - Pager number or Pager e-mail address
 - Pager service provider
- 5 Click **Modify Contact Data**.

To set the device priority:

- 1 Open a Network Map session.
- 2 Find your core device and select it.
- 3 Click **Object > Device Properties**.
- 4 In the Device Properties window, make this device priority 6.
- 5 Click **Apply**.
- 6 Click **OK**.

You have now changed the priority of your core device to 6.

To set up the event filter:

- 1 Click **Administration > Event filter configuration > Add a device filter**.
- 2 Enter the event filter information as it appears in this table:

Table 3 Example 1 Input

Field	Enter:
Name (create a name for the filter)	core_device_broken
Description	Page administrator when core device breaks
Event Type	Attribute
Attribute Group	Breaks
Priority	6

Table 3 Example 1 Input

Field	Enter:
Device Type	ATM Switch
Transitions	OK to Minor, OK to Major, OK to Critical, Minor to Major, Minor to Critical, Major to Critical
IPv4 Range	Select the devices or IP range you want this event filter to monitor
Alphanumeric Page	Select the Administrator account

- 3 You can have Enterprise Discovery delay the notification by entering a time in the Delay section of the notification table.
- 4 Click **Add Filter**.

Name: core_device_broken
Description: Page the administrator when a core device breaks

Selection Criteria

Event Type:	Attribute Group:	Priority:	Device Type:
<input type="checkbox"/> All <input checked="" type="checkbox"/> Attribute <input type="checkbox"/> Adds <input type="checkbox"/> Deletes <input type="checkbox"/> Moves	<input type="checkbox"/> All <input type="checkbox"/> Disk <input type="checkbox"/> Packet Loss <input checked="" type="checkbox"/> Breaks <input type="checkbox"/> Backplane Utilization	<input type="checkbox"/> All <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input checked="" type="checkbox"/> 6	<input type="checkbox"/> All <input type="checkbox"/> Enterprise Switch Layer 2 or below <input checked="" type="checkbox"/> ATM Switch <input type="checkbox"/> Ethernet/100 Hub <input type="checkbox"/> FDDI

State Transition:	From State	To State	Action	StateTransition
	n/a Ok Info Minor Major Critical	--> n/a Ok Info Minor Major Critical	Add Remove	OK to Minor OK to Major OK to Critical Minor to Major Minor to Critical Major to Critical
				Select All

Add by Interval

Starting IPv4 Address:
Ending IPv4 Address:

Add

Added IPv4 Ranges

172.22.1.253 to 172.22.1.253 (1 devices)

Delete

IPv4 Range:

Add by Subnet

IPv4 Address:
Netmask:

Add

Notification

E-mail:

<input type="checkbox"/> admin (Administrator)
<input type="checkbox"/> aggregator
<input type="checkbox"/> demo (Demo Account)

Delay: Hours: 0 Minutes: 0 Seconds: 0

Alphanumeric Page
(via e-mail gateway):

<input checked="" type="checkbox"/> admin (Administrator)
<input type="checkbox"/> aggregator
<input type="checkbox"/> demo (Demo Account)

Delay: Hours: 0 Minutes: 0 Seconds: 0

SNMP Trap:

<input type="checkbox"/> admin (Administrator)
<input type="checkbox"/> aggregator
<input type="checkbox"/> demo (Demo Account)

Delay: Hours: 0 Minutes: 0 Seconds: 0

Xml:

☐ On ☒ Off

Delay: Hours: 0 Minutes: 0 Seconds: 0

Add Filter

Example 2: Notification when a router is dropping a lot of traffic

This example shows how to create an event filter that will notify you (or someone else with an Administrator account) by e-mail message when your priority 6 routers have packet loss alarms.

To set up the Administrator account:

- 1 Click **Administration > Account administration > Account contact data**.
- 2 Select the Administrator account that you want to change.
- 3 Click **Modify Properties**.
- 4 Enter the correct e-mail address.
- 5 Click **Modify Contact Data**.

To set the device priority:

- 1 Open a Network Map session.
- 2 Find your Router and select it.
- 3 Click **Object > Device Properties**.
- 4 In the Device Properties window, make this device priority 6.
- 5 Click **Apply**.
- 6 Click **OK**.

If you want to set this up for several routers, then repeat these steps for each router. Note their IPv4 addresses if you want to specify the IPv4 range.

- 7 Set the Packet Loss thresholds by clicking **Edit > Alarm Thresholds**.
- 8 Click **Apply**.
- 9 Click **OK**.

To set up the Event Filter:

- 1 Click **Administration > Event filter configuration > Add a device filter**.
- 2 Enter the event filter information as it appears in this table:

Table 4 Example 2 Input

Field	Enter:
Name (create a name for the filter)	routers_dropping_traffic
Description	E-mail me when routers are dropping a lot of traffic
Event Type	Attribute
Attribute Group	Packet Loss
Priority	6
Transitions	OK > Minor, OK > Major, OK > Critical, Minor > Major, Minor > Critical, Major > Critical

Table 4 Example 2 Input

Field	Enter:
Device Type	Router
E-mail	select the Administrator account
IPv4 Range	Select the devices or IP range you want this event filter to monitor

3 Click Add Filter.

Name:

Description:

Selection Criteria

Event Type: ☐ All ☒ Attribute ☐ Adds ☐ Deletes ☐ Moves

Attribute Group: ☐ All ☐ UISK ☒ Packet Loss ☐ Breaks ☐ Backplane Utilization

Priority: ☐ All ☐ 3 ☐ 4 ☐ 5 ☒ 6

Device Type: ☐ All ☐ Discovery Server ☐ Cloud ☒ Router ☐ Workstation

State Transition:

From State	To State	Action	StateTransition
n/a	n/a	<input type="button" value="Add"/>	OK to Minor
Ok	Ok	<input type="button" value="Remove"/>	OK to Major
Info	Info		OK to Critical
Minor	Minor		Minor to Major
Major	Major		Minor to Critical
Critical	Critical		Major to Critical

Add by Interval

Starting IPv4 Address:

Ending IPv4 Address:

Added IPv4 Ranges

172.22.1.79 to 172.22.1.251 (173 devices)
172.22.2.2 to 172.22.5.56 (823 devices)

Add by Subnet

IPv4 Address:

Netmask:

Notification

E-mail: ☒ admin (Administrator) ☐ aggregator ☐ demo (Demo Account) Delay: Hours: Minutes: Seconds:

Alphanumeric Page (via e-mail gateway): ☐ admin (Administrator) ☐ aggregator ☐ demo (Demo Account) Delay: Hours: Minutes: Seconds:

SNMP Trap: Delay: Hours: Minutes: Seconds:

Xml: ☐ On ☒ Off Delay: Hours: Minutes: Seconds:

Example 3: Notify me when a line to an important device has long delays

This example demonstrates how to set up an event filter that will e-mail you when a line has delay alarms. Line event filters are a little more complex than device event filters, because you must select both a device, and the type of line connected to that device. For this example, we will use a server connected to a half duplex Ethernet line of 10Mbps or less (Ethernet 10< HD).

To set up the Administrator account:

- 1 Click **Administration > Account administration > Account contact data**.
- 2 Select the Administrator account that you want to change.
- 3 Click **Modify Properties**.
- 4 Enter the correct e-mail address.
- 5 Click **Modify Contact Data**.

To set the device priority:

- 1 Open a Network Map session.
- 2 Find your server and select it.
- 3 Click **Object > Device Properties**.
- 4 In the Device Properties window, make this Server priority 6.
Lines get their priority from the highest priority devices they connect. By making this device a priority 6, the lines attached to it are automatically a priority 6.
- 5 Click **Apply**.
- 6 Click **OK**.
If you want to be paged for several servers, repeat steps 2-6 for each server.
- 7 Set the Line Alarm thresholds by clicking **Edit > Alarm Thresholds**.
- 8 Click **Apply**.
- 9 Click **OK**.

To set up the Event Filter:

- 1 Click **Administration > Event filter configuration > Add a line filter**.
- 2 Enter the event filter information as it appears in this table:

Table 5 Example 3 Input

Field	Enter:
Name (create a name for the filter)	server_delays
Description	E-mail me when server lines have Delay alarms
Event Type	Attribute
Attribute Group	Delays
Priority	6

Table 5 Example 3 Input

Field	Enter:
Device Type	Server
Line Alarm Type	Ethernet 10< HD
Transitions	OK > Minor, OK > Major, OK > Critical, Minor > Major, Minor > Critical, Major > Critical
E-mail	select the Administrator account
IPv4 Range	Select the devices or IP range you want this event filter to monitor

3 Click **Add Filter**.

Name:

Description:

Selection Criteria

Event Type:	Attribute Group:	Priority:	Device Type:	Line Alarm Type:
<input type="checkbox"/> All <input checked="" type="checkbox"/> Attribute <input type="checkbox"/> Adds <input type="checkbox"/> Deletes <input type="checkbox"/> Moves	<input type="checkbox"/> All <input type="checkbox"/> Data Delivery Ratio <input type="checkbox"/> Frame Delivery Ratio <input checked="" type="checkbox"/> Delay <input type="checkbox"/> Line Utilization	<input type="checkbox"/> All <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input checked="" type="checkbox"/> 6	<input type="checkbox"/> All <input type="checkbox"/> Unmapped IP <input type="checkbox"/> Unknown NCD <input checked="" type="checkbox"/> Server <input type="checkbox"/> Printer	<input type="checkbox"/> All <input type="checkbox"/> Generic HD <input type="checkbox"/> Generic FD <input checked="" type="checkbox"/> Ethernet 10< HD <input checked="" type="checkbox"/> Ethernet 10< FD

State Transition:	From State	To State	Action	StateTransition
	n/a Ok Info Minor Major Critical	--> n/a Ok Info Minor Major Critical	<input type="button" value="Add"/> <input type="button" value="Remove"/>	OK to Minor OK to Major OK to Critical Minor to Major Minor to Critical Major to Critical <input type="button" value="Select All"/>

Add by Interval

Starting IPv4 Address:

Ending IPv4 Address:

Added IPv4 Ranges

172.22.1.79 to 172.22.1.251 (173 devices)
172.22.2.2 to 172.22.2.56 (55 devices)

IPv4 Range:

Add by Subnet

IPv4 Address:

Netmask:

Notification

E-mail:	<input checked="" type="checkbox"/> admin (Administrator) <input type="checkbox"/> aggregator <input type="checkbox"/> demo (Demo Account)	Delay: Hours: <input type="text" value="0"/> Minutes: <input type="text" value="0"/> Seconds: <input type="text" value="0"/>
Alphanumeric Page (via e-mail gateway):	<input type="checkbox"/> admin (Administrator) <input type="checkbox"/> aggregator <input type="checkbox"/> demo (Demo Account)	Delay: Hours: <input type="text" value="0"/> Minutes: <input type="text" value="0"/> Seconds: <input type="text" value="0"/>
SNMP Trap:	<input type="text"/>	Delay: Hours: <input type="text" value="0"/> Minutes: <input type="text" value="0"/> Seconds: <input type="text" value="0"/>
Xml:	<input type="radio"/> On <input checked="" type="radio"/> Off	Delay: Hours: <input type="text" value="0"/> Minutes: <input type="text" value="0"/> Seconds: <input type="text" value="0"/>

Index

A

- alarm thresholds
 - changing, 39, 43
 - copy and paste values, 41
 - device types, 39
 - line alarm types, 40
- ATM cells, 10
- Attribute Manager
 - Statistics, 37

B

- Backplane Utilization, 13
- Breaks
 - Line see Line Breaks
- Broadcasts, 11, 27
- broken line see Line Breaks

C

- capacity, line, 9
- Collisions, 11, 27, 34
- comma separated value *see* CSV
- copy
 - alarm thresholds command, 41
- CPU Utilization, 13
- CSV, 31, 33, 36, 37

D

- default map configuration, 31, 32
- Delay, 11, 27
- Device Breaks, 27
- Device Manager
 - Export (Statistics), 34
 - Graph (Statistics), 34
 - State, 33
 - Statistics, 33 to 35
 - Table (Statistics), 34
- Device Moves, 14
- Device MTBF, 14

- Device MTTR, 14
- Device Reports, 31
- device types, 39
- Disk Utilization, 13

E

- Errors, 12, 27
- event filters
 - examples, 44
- Executive/Summary Reports, 24
- Export
 - Device Manager Statistics button, 34

F

- frame relay, 12

G

- Graph
 - Device Manager button, 34
- gray background
 - Manager data, 33, 36

H

Health Panel

- Backplane Utilization, 13
- Broadcasts, 11
- Collisions, 11
- CPU Utilization, 13
- Delay, 11
- Device Moves, 14
- Device MTBF, 14
- Device MTTR, 14
- Disk Utilization, 13
- Errors, 12
- Frame Relay, 12
- Line Breaks, 9
- Load Average, 13
- Memory Utilization, 13
- Packet Loss, 12
- Port Moves, 14
- Port MTBF, 14
- Port MTTR, 13
- Printer, 13
- UPS, 13
- Utilization, 9

L

LAN Reports, 30

line alarm types, 40

Line Breaks, 9, 27

line capacity, 9

Load Average, 13

M

mean peak statistics, 23

mean statistic, 23

Memory Utilization, 13

N

negative statistics, 33, 36

P

Packet Loss, 12, 27

paste

- alarm thresholds command, 41

peak statistics, 23

period, sampling, 12, 14

Port Manager

- State, 36

Port Moves, 14

Port MTBF, 14

Port MTTR, 13

Printer, 13

R

recorded events

- Backplane Utilization, 13
- Broadcasts, 11
- Collisions, 11
- CPU Utilization, 13
- Delay, 11
- Device Moves, 14
- Device MTBF, 14
- Device MTTR, 14
- Disk Utilization, 13
- Errors, 12
- Frame Relay, 12
- Line Breaks, 9
- Load Average, 13
- Memory Utilization, 13
- Packet Loss, 12
- Port Moves, 14
- Port MTBF, 14
- Port MTTR, 13
- Printer, 13
- UPS, 13
- Utilization, 9

Reports

business

- device, 31
- executive/summary, 24
- LAN, 30
- WAN, 28
- statistics, 23

S

sampling period, 12, 14

spreadsheets, exporting to. *See* CSV

stale data, 33, 36

State panel

- Device Manager, 33
- Port Manager, 36

Statistics

- Attribute Manager panel, 37
- Device Manager panel, 33 to 35

T

Table

- Device Manager button, 34

- thresholds
 - alarm
 - changing, 39, 43
 - device, 39
 - line alarms, 40

U

- UPS, 13

- Utilization, 9

W

- WAN Reports, 28

