Peregrine

Network Discovery

Reference Manual

Peregrine
SYSTEMS®

PART NO: PND-5.0.2-ENG-01003-00296

Copyright information is continued in *Appendix B, Copyright*.

This document and the related software described in this manual are supplied under license or nondisclosure agreement and may be used or copied only in accordance with the terms of the agreement. The information in this document is subject to change without notice and does not represent a commitment on the part of Peregrine Systems, Inc. Contact Peregrine Systems, Inc., Customer Support to verify the date of the latest version of this document.

The names of companies and individuals used in the sample database and in examples in the manuals are fictitious and are intended to illustrate the use of the software. Any resemblance to actual companies or individuals, whether past or present, is purely coincidental.

If you need technical support for this product, or would like to request documentation for a product for which you are licensed, contact Peregrine Systems, Inc. Customer Support by e-mail at support@peregrine.com.

If you have comments or suggestions about this documentation, contact Peregrine Systems, Inc. Technical Publications by e-mail at doc_comments@peregrine.com.

This edition applies to version 5.0.2 of the program, Peregrine's Network Discovery.

Peregrine Systems, Inc.
Worldwide Corporate Headquarters
3611 Valley Centre Drive San Diego, CA 92130
Tel 800.638.5231 or 858.481.5000
Fax 858.481.1751
www.peregrine.com

Reference Manual

Table of Contents

Introducing Network Discovery

Network Discovery is a Web-based tool for continuous network discovery, visualization, and management. Network Discovery ™ identifies, monitors, and collects information for every device in your network.

Even with today's complex and volatile networks, Network Discovery:

- Enhances tactical and strategic decision making by providing real-time network views, statistics, and forecasts;
- Complements your existing network infrastructure by delivering cost-effective, easy-to-deploy network management capabilities not previously available;
- Maximizes your asset management and service desk programs by providing complete and accurate inventory.

The Network Discovery documentation set includes the following:

- *Network Discovery Setup Guide*
- *Network Discovery Reference Manual*
- *Network Discovery User Guide*
- *Network Discovery Data Export Guide*
- *Network Discovery Release Notes*

To contact Peregrine Systems, refer to *Appendix A, Need more help?*.

Certain chapters of this *Reference Manual* are useful only to customers who have purchased certain modules or features of Network Discovery. All other customers may safely ignore these chapters.

Aggregator

Customers who have purchased multiple Peregrine appliances and who have enabled one Peregrine appliance to act as an Aggregator should make sure they read the following chapters:

- *Chapter 4, Aggregate Toolbar and Other Navigation*
- *Chapter 6, Aggregate Health Panel*
- *Chapter 8, Remote Appliances*
- *Chapter 20, Administration for Administrator Accounts*; section *Remote Appliance Administration* on page 327

For a detailed introduction, see *Aggregator* on page 29.

This *Reference Manual* is about Network Discovery software. for information on hardware specifications or installation, see the *Network Discovery Setup Guide*.

CHAPTER 2

Terms and Concepts

- To review terms and concepts common to network management, see *Network Terms and Concepts* on page 18.
  - *Domain names* on page 18
  - *Address types* on page 18
  - *Netmask notation* on page 19
  - *Community strings* on page 20
  - *Bridge aging* on page 20
  - *OSI model layers* on page 21
  - *Management workstation* on page 21
- To learn terms and concepts unique to this product, see *Network Discovery Terms and Concepts* on page 22.
  - *Objects* on page 22
  - *Packaging* on page 25
  - *Device identification* on page 26
  - *Aggregator* on page 29
  - *Poll cycle and sampling period* on page 27
  - *Priority* on page 28
  - *Account types* on page 31
  - *Removal of devices* on page 34
  - *Special input syntax* on page 36

Related

- See also *Appendix C, Glossary of Abbreviations* on page 401.
- To read an overview, see *Chapter 21, How Network Discovery Works* on page 381.

Network Terms and Concepts

These terms and concepts are common to networks and network management. They are not unique to Network Discovery ™.

Domain names

Example: website.example.com

A domain name such as “website.example.com” is easier to remember than an IP address such as “192.168.96.1”. This ease of remembering is the chief reason for the existence of domain names.

The term “domain name” and “host name” are sometimes used interchangeably. A domain name is a name in the Domain Name System (DNS) format as registered with a DNS server. A host name is purely an internal name, used by a device to refer to itself.

Address types

The two main types of numeric address are the IP address and the MAC address.

IP address

An IP address was intended to be a unique number identifying a unique device or port of a device.

When you see the term “IP address” with no qualifiers in Network Discovery, it means that either an IPv4 address or an IPv6 address is acceptable. The 32-bit address space of IPv4 addresses puts severe limits on the number of unique addresses available, and the supply is fast running out. The IPv6 128-bit address space was created to address this problem.

IPv4 address

An IPv4 address contains four sections separated by periods (or “dots”). Each section, called an octet, contains 8 bits expressed in decimal (0–255).

Example: 192.168.96.1

IPv6 address

An IPv6 address contains eight sections separated by colons. Each section contains 16 bits expressed in hexadecimal (0000–FFFF).

Example: 1234:5678:9ABC:DEF0:1234:5678:9ABC:DEF0

To make it easier to remember and type an IPv6 address, you can use a double colon (::) to indicate multiple contiguous sections of zeros. You can also omit leading zeroes. For example, you can simplify address 0123:0000:0000:0000:0004:0056:789A:BCDE to 123::4:56:789A:BCDE.

MAC address

A MAC address is a unique number identifying a unique device or port of a device in an Ethernet network.

When you see the term “MAC address”, it means a numeric MAC address.

Numeric MAC address

A MAC address contains six sections. Each section contains 8 bits expressed as a hexadecimal number (00–FF).

Sometimes the first three sections and last three sections are separated by one space; sometimes all sections are presented as one, without spaces; sometimes each section is separated by a colon or a space.

Examples: 010203 FDFEFF, 010203FDFEFF, 01:02:03:FD:FE:FF

MAC address including OUI

This type of MAC address is sometimes (inaccurately) referred to simply as an OUI. In fact, the Organization Unique Identifier (OUI) comprises the first three sections of a MAC address. If Network Discovery recognizes the numeric form of the OUI, it replaces the numbers with a short form of the organization name. This makes it easier to identify a device. If Network Discovery uses an alphabetic short form for a device’s OUI, the device is said to have a recognized OUI. Having a recognized OUI is sometimes abbreviated to “having” an OUI.

Example: DELL 59FC91

Netmask notation

Network masks, often referred to as netmasks, can usually be expressed in two formats in IPv4—either the familiar octet notation (also called dotted decimal notation) or CIDR notation.

Example of octet notation: 255.255.255.248

Example of CIDR notation: 29

The shorter CIDR notation is based on the binary equivalent of the octet notation, and refers to the numbers of contiguous 1’s.

Table 1: Example netmask notation—octet and CIDR

255.255.255.255	11111111.11111111.11111111.11111111	32 1’s
255.255.255.248	11111111.11111111.11111111.11111000	29 1’s
255.255.0.0	11111111.11111111.00000000.00000000	16 1’s

In IPv6, netmasks can only be written in CIDR notation.

Community strings

A community string is a kind of device-based password that controls access to the SNMP MIB of a device. A device controls its own community strings, but you must tell Network Discovery about them.

If Network Discovery is not given the correct community strings and access to devices on your network, Network Discovery will be unable to read device MIBs. Network Discovery will then assume that each device it cannot read has no SNMP management available.

With directed community strings, the device not only stores a "password", but a list of trusted devices. If the Peregrine appliance is not on the list of trusted devices, the device will not recognize Network Discovery and Network Discovery will fail to read the device's MIB—even though Network Discovery knows a valid string. Therefore, it is not enough to configure Network Discovery to know about your network devices. You must also configure your network devices to know about the Peregrine appliance.

Bridge aging

To obtain the best results with Network Discovery, turn bridge aging on. Also, set the aging interval for 2–6 hours, although some circumstances may call for an aging interval as long as 12 or even 24 hours. (Longer aging intervals are not always possible. A common maximum aging interval is 32767 seconds, or just over 9 hours.)

Bridges, routers, and switches generally have tables in which they store the addresses of devices on the network. The tables are periodically purged and relearned in order to keep the list of devices current. The aging interval defines the frequency with which tables are purged and relearned.

When there is no table entry for the address of an incoming packet, the bridge, router, or switch must learn the location of the address. To learn the location, the device sends the incoming packet to all its own ports. (This is often referred to as "flooding" or "leakage".) When the destination device with the corresponding address responds, the bridge, router, or switch learns the location and makes an entry in the address table.

If the table is full and a new entry must be made, the "oldest" entry is usually replaced by the new entry. Device manufacturers commonly strive to include a table large enough to hold the addresses of all active sessions, but space in a table is always finite.

Network Discovery reads the tables of bridges, routers, and switches to learn the addresses of all the connected devices. Many bridge, router, and switch vendors use a standard aging interval of 300 seconds (5 minutes), which is too short.

If the bridge aging interval is too short:

- Network Discovery may never discover devices that are connected to the network for short periods—for example, laptops.
- Network Discovery may take longer to determine connections between devices that it has discovered.
- Tables will be purged so frequently that flooding will occur regularly, using bandwidth unnecessarily.

If bridge aging is not turned on for a device, or if the bridge aging interval is too long:

- Tables will contain old addresses of devices that may been removed from the network or devices that are broken. As a result, Network Discovery will work from an outdated and possibly confused representation of what is in your network and how it is connected.

OSI model layers

The Open Systems Interconnection (OSI) model has seven layers. Layers 2 and 3 are the most important to Network Discovery:

- Layer 2 is the Data Link layer, at which level MAC addresses are used. Bridges and some switches are layer 2 devices.
- Layer 3 is the Network layer, at which level IP addresses are used. Routers are layer 3 devices.

Some switches are both layer 2 and layer 3.

The seven layers are:

Layer number	Layer
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Management workstation

Any workstation or personal computer capable of running a supported web browser (Netscape 6.07 or later; Microsoft Internet Explorer 5.0 or later). There is more detail on requirements for a management workstation in the *Setup Guide*.

Note: Java and JavaScript must be enabled in order for Network Discovery to work properly.

Note: Internet Explorer 5 requires Microsoft VM build 3193 or later. The VM is not automatically upgraded when you set up IE5.

Network Discovery Terms and Concepts

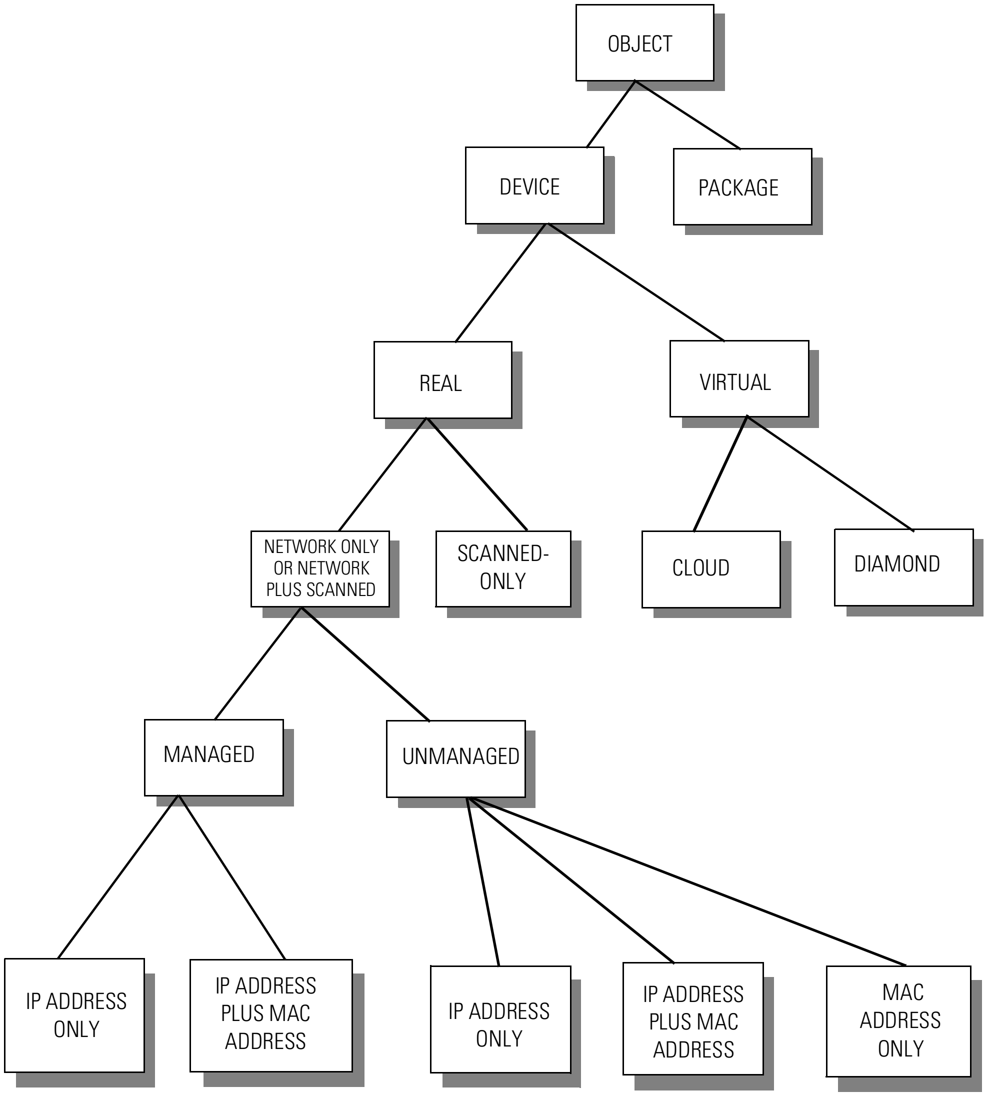
These terms and concepts are either unique to Network Discovery, or have a special meaning in this context.

Objects

A map displays icons and lines. Icons represent objects. Objects comprise devices and packages.

(Two sorts of objects are not displayed on a map—ports and attributes.)

Figure 2-1: Object type hierarchy



Devices

Devices come in two classes, real and virtual.

Devices also come in two connectivity classes, network connectivity devices (NCDs) and end nodes. Connectivity class is discussed under *Packages* on page 24.

Real devices

Real devices are devices that Network Discovery can positively identify and assign a device type. The device type as identified by Network Discovery corresponds to the device icon assigned by Network Discovery.

Network Discovery finds a Network device automatically, in one of three ways:

- the device responds when Network Discovery pings its IP address
- information from the device appears in a table:
  - the IP address in a router's ARP tables
  - the MAC address in a switch's bridge table
- the MAC address of the device appears in a concentrator's or hub's Source Address capture

Scanned devices are found when the WMI Collector sends their scan files to the Peregrine appliance.

Network devices can be SNMP-managed or unmanaged:

- SNMP-managed device: a device with SNMP information from the network (may also contain scan data)
- Unmanaged device: a device with no SNMP information from the network (may also contain scan data)
  - MAC+IP device: an unmanaged device with a MAC address and an IP address
  - IP-only device: an unmanaged device with no MAC address and no scan data
  - MAC-only device: an unmanaged device with no IP address and no scan data

A scanned-only device is a device with scan data for which there is not yet any information from the network. Scan data is collected by Peregrine's Express Inventory, the WMI Collector. For more information on setting up and using the WMI Collector, see your Service Center Essentials documentation.

Virtual devices

Virtual devices are principally connectivity tools. When Network Discovery has determined that two devices are somehow connected but cannot be certain of the exact path of the connection, it inserts a virtual device between the two network devices, as a sort of placeholder. The placeholder represents either an unidentified device, or an unidentified connection between devices.

Virtual devices come in two types: the cloud and the diamond. The cloud is used to represent a real device or group of real devices that Network Discovery cannot yet identify. The diamond is used to represent connectivity that Network Discovery has not yet determined. Since a diamond is an object that does not usually represent an object, the diamond is more theoretical than a cloud.

Packages

Packages are groups of objects. You use packages to simplify the viewing and visualization of a map. Clicking a package icon reveals the contents of the package in a separate map window.

Devices come in two connectivity classes, network connectivity devices (NCDs) and end nodes. These two types are packaged differently.

A network connectivity device, such as a router or switch, establishes connectivity within your network. An end node, such as a printer or workstation, is connected to only one other device, and has a single connection to that device. Such a device appears at the end of a line.

Network Discovery automatically creates end node packages. Users can create packages of both connectivity classes (that is, not just end nodes), or can request that Network Discovery create these types of packages.

Packaging

The concept of a package as an object is discussed (briefly) above in *Packages*, and in greater detail in *Packages* on page 124. This section addresses the process of packaging and unpackaging.

There are two types of packaging processes. The first is automatic packaging, done by Network Discovery in response to the settings of **Administration** > **Display Preferences** > **Automatic Packaging** (*Automatic Packaging* on page 372). Automatic packaging affects end nodes. The second is manual packaging, which a user requests. Manual packaging can be semi-automated, through the use of the *Pack* command. The user can also have more control of the packaging process by using the *Create Package*, *Package*, *Unpackage*, and *Promote* commands.

All objects have a packaging status. They are either locked or unlocked. By default, objects are unlocked. You lock an object to prevent automatic packaging.

Effects of manual packaging

Once an object is locked, Network Discovery no longer automatically does any automatic packaging on it. Specifically, Network Discovery no longer:

- packages the object
- unpackages the object
- destroys the package containing the object

Locked objects may still be packaged manually, by the user. Locked objects may also be unlocked manually.

Sometimes manually packaging an object has unexpected effects. For example, a single device may remain unpackaged when all others around it are packaged. When packaging status is made visible, the reason for the lone unpackaged device often becomes obvious.

How an object can become locked

You can lock an object with the *Lock* command. You also lock an object as a side effect of doing any manual packaging. That is, using the commands *Package*, *Unpackage*, or *Promote* can cause objects to become locked. You cause an object to be locked, most commonly, when you move an object into or out of a end node package.

The rationale is this: It would be very confusing and frequently counterproductive if objects that you deliberately packaged were then automatically unpackaged by Network Discovery.

How to unlock an object

You unlock an object by using the *Unlock* command. You unlock all objects by using the *Unpack All* command.

In some circumstances, promoting objects—particularly into the Main Map window—will also unlock the objects.

Visibility of packaging status

Packaging status refers to whether an object is locked or unlocked as far as packaging operations are concerned. The packaging status of objects can be made visible or invisible by using the *Underline Locked Objects* command (for temporary change) or the *Underline locked objects* option (for permanent change).

A blue line underneath an icon indicates that an object is locked. By default, this blue line is not shown.

Related

- *Lock* on page 161 and *Unlock* on page 162
- *Unpackage* on page 163 and *Package* on page 164
- *Promote* on page 164
- *Automatic Packaging* on page 372
- The account preference *Underline locked objects* on page 145
- The command *Underline Locked Objects* on page 152

Device identification

For details, see **Help** > **Device Types**.

Icons

Icon assignment is based on device type as determined by Network Discovery.

Note: Changing a device's icon also changes its type.

Device type represents the first level of device identification. It classifies each device to a greater or lesser degree.

Examples: router, ATM switch, Microsoft workstation

Devices have a connectivity class:

- Network connectivity device
- End node
- Unknown

Network connectivity devices, such as routers and switches, establish connectivity within your network. An end node, such as a printer or workstation, is connected to only one other device, and has a single connection to that device. Such a device appears at the end of a line.

End node devices have a device class:

- Server
- Workstation
- I/O
- Miscellaneous
- Unknown
- Cloud

Tags

Device tags represent the second level of device identification. They describe the device series, model, brand, or manufacturer.

Examples: Cisco 1601, Windows 98.

The device tag is the first available of:

- Rule-specific tag
- Model
- Family
- Application
- Operating System (OS)
- Registered SysObjectId Manufacturer
- Registered OUI(MAC) Manufacturer

The rule-specific tag is employed when only limited information is available (such as the organization number within a SysObjectId, MAC address, host name), or when a managed device is not listed in the Network Discovery Rulebase and a generic or low level rule is used to identify the device.

If the probability of device identification is less than 90%, the tag ends with "?". If the device is likely an end node but may be a Network Connectivity Device (NCD), the rule-specific tag contains "NCD?" at the end.

Virtual devices do not have tags.

Package tags display the number of devices contained by the package.

Poll cycle and sampling period

To ensure that you have up-to-date information about your network, Network Discovery continually polls every device in your network, one by one. This is called a poll cycle. The time that it takes to complete one poll cycle is called the sampling period.

You can easily observe the progress of the poll cycle if you have a map window open. At the bottom of each map window is a status bar. On the right of the status bar is a progress bar. When the progress bar is completely white, a poll cycle has just begun. When the progress bar is completely gray, a poll cycle has just ended.

You can also have your Peregrine Systems Customer Support representative calculate the poll cycle for you.

Priority

In Network Discovery, each object and line on the Network Map has a priority.

Devices and lines can have priorities 1–6. Devices and lines with priority 1 are the least important. The higher the number, the higher the priority and greater the importance.

The highest priority that Network Discovery assigns is 4. The highest priority that the user can assign is 6.

Devices

When Network Discovery identifies a device, it assigns a priority to the device. All users can change the priority of a device.

Table 2: Priority of objects

Default		Example	Notes
more important			
6	—	user-assigned only	default e-mail notification
5	—	user-assigned only	—
4	Network-connectivity objects	switches, hubs, routers, gateways, clouds	—
3	Servers	—	—
2	Common-use and auxiliary devices	printers, analyzers, UPSes	—
1	Workstations	—	—
less important			

By default, only devices and lines with priority 6 in the Prime configuration generate an e-mail notification of break fault events. To change this, see *Event Filter Configuration* on page 337.

Only the device priority from the Prime configuration affects event e-mail and pager notification.

For priorities assigned to specific icons, see **Help** > **Device Types**.

Lines

A line inherits its priority from the devices it connects. The device with the lower priority determines the priority for the line. You can only change the priority of a line by changing the priority of the devices at its endpoints.

Packages

A package takes its priority from the highest device it contains. For example, a package containing several priority 1 devices and only one priority 6 device has a priority of 6.

Aggregator

Important: This section is only of interest if you have multiple Peregrine appliances in your network.

If your network is larger than a single Peregrine appliance can accommodate, you can use an Aggregator to present a summary view of all Peregrine appliances.

An Aggregator is an ordinary Peregrine appliance with a special license that can collect and display data from multiple Peregrine appliances. It imports Health Panel data and Events from other appliances (called “remote appliances”).

Any Peregrine appliance can be used as an Aggregator appliance by the application of an Aggregator license. Also, any Peregrine appliance can be a source for an Aggregator—no license is required.

Only a single Aggregator is needed. Each Aggregator appliance can have as many as five remote appliances.

An Aggregator has three principal benefits. You have:

- an overview of all Peregrine appliances via the Aggregate Health Panel and Aggregate Events Browser
- a quick and easy way to administer all Peregrine appliances without having to log in to each (one Toolbar for all Peregrine appliances)
- an integrated data source for export onto data access applications using the Open Database Connectivity Standard (ODBC)

The Aggregate Health Panel displays the alarms and warnings from the multiple Peregrine appliances.

There is currently no aggregation of the Network Map, the Service Analyzer, the Reports, or Find. Neither are the Status or Administration menus aggregated.

However, there are shortcuts in the Network Map that allow you to quickly view maps from multiple remote appliances (provided the Aggregator appliance has been configured to produce a correct map for the Aggregator itself). A special right-click menu is available for Peregrine appliances—see *Device* on page 170.

There are also navigation shortcuts in two flavors: one for users who prefer to navigate with the Toolbar and one for users who prefer the navigational hyperlinks. These shortcuts allow you to see the contents of your remote appliances and administrate your remote appliances without having to log in separately to each appliance.

Important: There can be duplicate devices. The Aggregator does not eliminate duplicates. If you have included a device in discovery ranges for more than one remote appliance, you will see that device appear multiple times in an Aggregate Health Panel report. (A report from a remote appliance is followed by the remote appliance’s name.)

If a remote appliance is not available, the Aggregator uses the last available imported Health Panel for that remote appliance. (Also, an unavailable remote appliance affects the display of the Appliances button.)

Customers who have purchased multiple Peregrine appliances and who have enabled one Peregrine appliance to act as an Aggregator should read the following chapters:

- *Chapter 4, Aggregate Toolbar and Other Navigation*
- *Chapter 6, Aggregate Health Panel*
- *Chapter 8, Remote Appliances*
- *Chapter 20, Administration for Administrator Accounts*; section *Remote Appliance Administration* on page 327

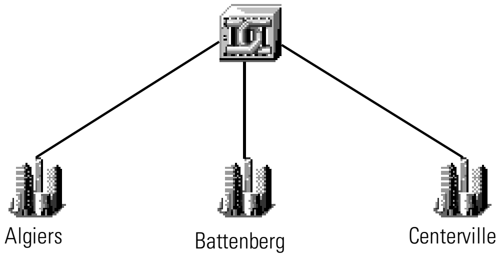
Recommended Set-up

There is more information on setting up an Aggregator in the *Setup Guide* and the *User Guide*, but in brief:

- add an IPv4 range for each remote appliance (**Administration** > **Network configuration** > **Add IPv4 range**)
- add an IPv4 range for each router

Suppose that you work with a business, ExampleCorp, that has offices in three cities: Algiers, Battenberg, and Centerville. Each office has 6,000 devices in its subnetwork.

Figure 2-2: Simple conceptual network map



Ideally, you would have purchased 4 Peregrine appliances: one for each office, and one to act as an Aggregator for the central office (in Centerville).

If you set up the Aggregator ranges to include only Peregrine appliances and routers, the resulting Network Map might look like this:

Figure 2-3: Network map with Peregrine appliances and routers

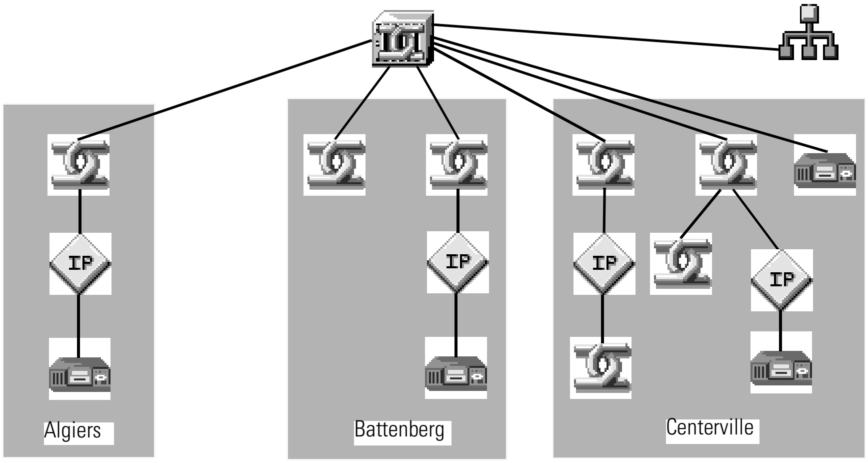


Figure 2-4: If the Network Map for your Aggregator does look like this, you can right-click on each Peregrine appliance to open map windows for each appliance. Right-click remote appliance > Network Map.

Account types

Network Discovery supports four types of account:

- Demo
- IT Employee
- IT Manager
- Administrator

Each account type has different permissions that affect access to areas of the product. Account type also affects the way in which some data is displayed, or even whether the data is displayed at all. Finally, account type affects the default settings of some aspects of Network Discovery.

The Network Discovery software comes with one of each type of account installed. If there are to be any other accounts, the owner of an Administrator account must create them. There can be as many as 250.

Table 2-1: Pre-installed accounts

Account type	Account name	Password
Demo	demo	demo
IT Employee	itemployee	password
IT Manager	itmanager	password
Administrator	admin	password

As many as six accounts can use a Network Map session at the same time.

To check how many people are using a map:

Click **Status** > **Network Map Sessions**. You see how many of the map sessions are currently available.

Table 3: Account types—permissions and displays

	Demo	IT Employee	IT Manager	Administrator
Network Map				
Initial map configuration file	Copy of Prime	Copy of Prime	Copy of Prime	Copy of Prime
Default map configuration file	Copy of Prime	last saved or used	last saved or used	last saved or used
Open any saved map configuration	YES	YES	YES	YES
Save any number of map configurations	YES	YES	YES	YES
Save a map configuration as Prime	—	—	YES	YES
Change a device icon	—	—	YES	YES
Change a package icon	YES	YES	YES	YES
Change a device’s priority	YES	YES	YES	YES
Change a device’s notification priority	—	—	YES	YES
Alarm Thresholds	view	view	view + change	view + change
Purge a device, a port or an attribute	—	—	YES	YES
Reset MTTR and MTBF for a device	—	—	YES	YES
Disconnect other accounts’ map sessions	—	—	—	YES
Managers (for example, Device Manager)				
View read and write community strings for device	—	—	YES	YES
View and use *set* link to MIB Browser	—	—	YES	YES
SNMP query default string	“public”	“public”	from Network Discovery	from Network Discovery
Update Model	—	—	YES	YES
Configure connections	—	—	YES	YES
Break and force connections	—	—	YES	YES
MIB Browser				
Set SNMP variables	—	—	YES	YES
Read community string	view	view + edit	view + edit	view + edit
Write community string	—	—	view + edit	view + edit
Status				
View read and write community strings for network	—	—	YES	YES
Administration				

	Demo	IT Employee	IT Manager	Administrator
Change own password	—	YES	YES	YES
Configure own account	—	YES	YES	YES
Configure other accounts	—	—	—	YES
Manage own map configurations	—	YES	YES	YES
Copy map configurations from other accounts	—	YES	YES	YES
Select pager service provider	—	YES	YES	YES
Configure pager service provider	—	—	—	YES
Configure event filters	—	—	—	YES
Configure Peregrine appliance	—	—	—	YES
Configure network operations	—	—	—	YES
Access to shared directory	read	read	read	read/write

IT Employee and IT Manager accounts share the same Administratio n capabilities

Demo accounts

Demo accounts are designed for training and practice. Demo is the least powerful type of account on Network Discovery. The restrictions on this account make it impossible for the Demo account owner to damage the network.

Initially, there is one Demo account. The name for this account is “demo” and the password is “demo” (account names must be lowercase and passwords are case-sensitive). Demo account owners cannot change this password. An Administrator account owner can create more Demo accounts if needed.

IT Employee accounts

For most day-to-day work with Network Discovery, an IT Employee account has the same capabilities as a Demo account. Neither of them can save a map configuration as Prime or choose a device’s icon, for instance. For Administration activities though, the IT Employee and IT Manager accounts are more similar. They can both change their own password, configure their own accounts and manage their own map configurations for example.

IT Manager accounts

The owner of an IT Manager account has the power to make changes that affect what other people see in Network Discovery.

In power, IT Manager accounts fall between IT Employee accounts and Administrator accounts. IT Manager accounts share the same capabilities as IT Employee accounts in Administration—neither can configure other accounts and neither does the setup tasks that the Administrator does. In all other respects—with one exception— IT Manager accounts have the same capabilities for day-to-day operations, as Administrator accounts. The exception is that IT Manager account users cannot disconnect other users’ map sessions.

With respect to the Administration menu, an IT Manager account has capabilities similar to an IT Employee account. With respect to the Network Map an IT Manager account is similar to an Administrator account.

Warning: There can be more than one Administrator and or IT Manager account. Two or more Administrator and or IT Manager users can access Network Discovery simultaneously. In this situation, there is a risk of one user overwriting the work of another user.

Administrator accounts

Warning: There can be more than one Administrator and or IT Manager account. Two or more Administrator and or IT Manager accounts can access Network Discovery simultaneously. In this situation, there is a risk of one account overwriting the work of another account.

There should be one Administrator account owner designated as the Network Discovery Administrator, whose account cannot be deleted. The default Administrator account name is “admin” and the default password is “password” (account names must be lowercase and passwords are case-sensitive). This is the most powerful type of account. Administrator accounts can access all components of the Peregrine appliance.

The pre-installed Administrator account must set up the initial Peregrine appliance parameters and create the other accounts. (See the *Setup Guide*).

Warning: If you forget the Administrator password, you will not be able to access the Administrator account without intervention from Peregrine Systems.

Removal of devices

Devices can be removed from your Network Map in one of two ways: automatic or manual.

Table 4: Device removal methods

Method	Performed by	Stages
automatic	Network Discovery	2 ■ trash ■ purge
manual	an IT Manager or Administrator user	1—purge only

Automatic

The automatic removal process begins once Network Discovery detects that a device has not been seen. The trash interval begins as soon as a device is discovered, and restarts after every model update. The length of this interval is specified in *Expiry* on page 352. When the trash interval ends, the device is moved into the trash.

Once the device is in the trash, the purge interval begins. The length of this interval depends is specified in *Expiry* on page 352. When the purge interval ends, the device is removed from the trash, and all associated data is removed from the database.

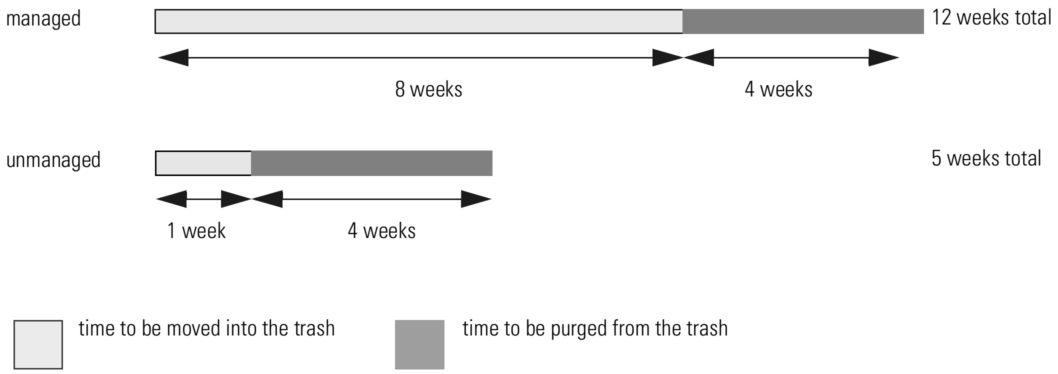
Table 5: Comparing trash and purge

Action	Trash	Purge
device removed from Network Map	YES	YES
device can be recovered if seen	YES	—*
“delete” event generated	YES	—
device statistics deleted	—	YES
device events deleted	—	YES

* Once purged, a device can still be rediscovered, but it will be considered a new device.

Note: The trash has limited capacity. Once trash capacity is exceeded, devices are purged, regardless of the trash interval. The number of devices that trash can hold is 10% of the device license for the Peregrine appliance.

Figure 2-5: Default values for automatic removal



Manual

The manual removal process begins when an Administrator user selects a device (in a map window **Object** menu or from the Device Manager). The device is immediately removed without being placed in the trash. (Manual removal may be accompanied by blocking the device, should the user choose.)

The manual removal of a device from the Network Map should be accompanied by its physical removal from the network, otherwise the device may reappear.

Note: If you change the address ranges in **Network configuration**, devices that are no longer included in the ranges are automatically put in the trash.

Special input syntax

You can create SNMP system variables for system name, system location, and system contact that will appear as hyperlinked within the Device Manager.

Network Discovery gives you a shorthand for entering URLs: “<URL: >”. You must include an appropriate prefix with the URL—such as “http://” or “mailto:”—or the link will not work.

Limits

Acceptable prefixes: mailto: | news: | http:// | https:// | telnet:// | ftp:// | gopher://

Table 6: URL syntax in system variables

	What you type	Results in Device Manager
CORRECT	sysadmin@example.com	sysadmin@example.com
CORRECT	<URL:mailto:sysadmin@example.com>	sysadmin@example.com
INCORRECT	<URL:sysadmin@example.com>	sysadmin@example.com*
INCORRECT	sysadmin@example.com (System Admin)	sysadmin@example.com (System Admin)*
CORRECT	<URL:mailto:sysadmin@example.com> (System Admin)	sysadmin@example.com (System Admin)
CORRECT	<URL:http://www.example.com>	http://www.example.com
CORRECT	http://www.example.com†	http://www.example.com
INCORRECT	<URL:www.example.com>	www.example.com*

* No text will be hyperlinked.

† Restricted to “http://” only. Not available to other prefixes.

3

CHAPTER

The Toolbar and Other Navigation

The Toolbar provides a way to navigate through Network Discovery. You may see one of two possible Toolbars:

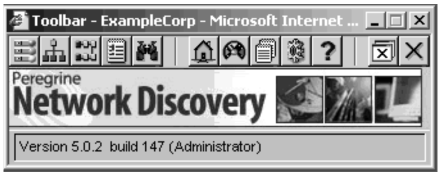
Figure 3-1: Toolbars

If your Toolbar looks like this:

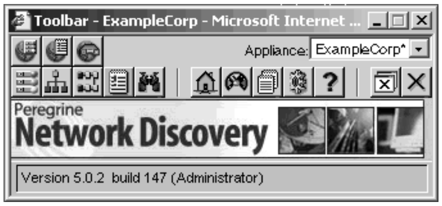
▶Consult this chapter.

If your Toolbar looks like this:

▶See *Chapter 4, Aggregate Toolbar and Other Navigation*



Version 5.0.2 build 147 (Administrator)



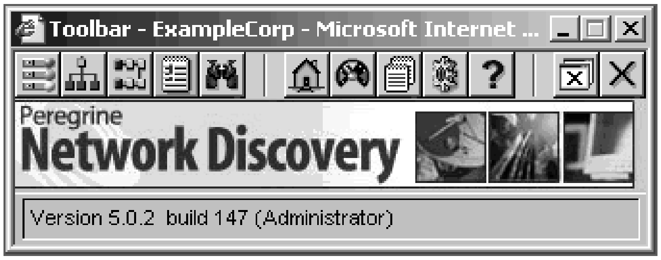
Appliance: ExampleCorp*

Version 5.0.2 build 147 (Administrator)

The main navigation buttons of the Toolbar are duplicated in the *Navigation Bar* on page 44, found as hyperlinks at the bottom of many Network Discovery pages.

Buttons

Figure 3-2: Toolbar



Version 5.0.2 build 147 (Administrator)

There are three groups of Toolbar buttons. The first group of buttons contains the major functions of Network Discovery.

Health Panel	Opens the Health Panel.	see *Chapter 5, Health Panel* and *Chapter 7, Health Panel Menus*
Network Map	Open the Network Map window. (To have the Health Panel open automatically as well, see *Open Health Panel with Network Map* on page 93.)	see *Chapter 9, Network Map Window* and *Chapter 10, Network Map Menus*
Service Analyzer	View end-to-end network performance.	see *Chapter 15, Service Analyzer*
Events Browser	View recent events.	see *Chapter 16, Events Browser*
Find	Search for devices and ports of devices.	see *Chapter 17, Find*

The second group of buttons uses the active web browser window.

Home	The Network Discovery home page.	see *Home* on page 40
Status	View configuration of the Peregrine appliance and of Network Discovery.	
Reports	View network statistics.	see *Chapter 18, Reports*

⌂	Home	The Network Discovery home page.	see *Home* on page 40
⚙	Administration	The function of this button depends on your account. ■ Demo users have no access to administration. ■ IT Employee users: Configure own account. ■ IT Manager: - Configure own account - Set appliance system variables ■ Administrator users: - Perform initial setup - Configure own and other accounts - Set appliance system variables - Set up Network Discovery	■ IT Employee and IT Manager users see *Chapter 19, Administration for IT Employee and IT Manager Accounts* ■ Administrator users see *Chapter 20, Administration for Administrator Accounts*
?	Help	Read documentation. This menu includes all manuals, release notes, and some quick-reference windows.	see *Help* on page 40

The third group of buttons controls your web browser environment.

☒	Close	Close all Network Discovery windows.	see *Close* on page 43
✕	Exit	Quit Network Discovery completely, but leaves any active web browser windows open.	see *Exit* on page 43

Status Window

The status window is a small text window at the bottom of the Toolbar. The status window displays three types of messages:

Table 1: Status window messages

Type	To view
version*/account†	point to any part of the Toolbar except the buttons
mini-help	point to any Toolbar button
loading progress	click the **Health Panel** or **Network Map** button; messages appear while Network Discovery loads the Health Panel or Network Map window

* If the version number ends in asterisk—for example, “5.0.0*”—then Network Discovery has been updated since it was installed from a CD.
† The full name associated with the account, if available; otherwise, the account name.

Default version/account

Home

The Home page welcomes you to Network Discovery. The menu on the Home page allows you to perform operations on the Peregrine appliance without using the Toolbar. Like the Toolbar, it gives access to the following main sections:

- Health Panel
- Network Map
- Service Analyzer
- Events Browser
- Find
- Status
- Reports
- Administration
- Help

In addition, it gives you access to the Download page.

Related

Because the Home page is the first page that you see after logging in to Network Discovery, the page also serves as an introduction to the *Navigation Bar* on page 44.

Help

The Help menu contains help pages available only in online versions, plus online versions of the main elements of the Network Discovery documentation set.

Table 2: Help menu elements

Help element	Availability
Manuals	
■*Setup Guide*	online and paper
■Data Export Guide	online and paper
■ *User Guide*	online and paper
■*Reference Manual*	online and paper
Release Notes	online and paper
Icons	online only
Exceptions	online only
Supported Device/Port Attributes	online only
Device Types	online only
Device Filters	online only
Device Title Filters	online only
Shortcuts	online only

Table 2: Help menu elements

Help element	Availability
About Network Discovery	online only
Peregrine Systems Customer Support—The Knowledge Base	online only

Ways of opening

- From the Toolbar, click the **Help** button.
- From the Health Panel or any map window, click the **Help** menu.

Manuals

Setup Guide

Online edition of the *Setup Guide*, which helps you learn how to install your Peregrine appliance and configure it for optimum exploration of your network.

Data Export Guide

Online edition of the *Data Export Guide*:

- explains what data is available from the Network Discovery database
- how to export Network Discovery data into CSV or XML format for use with Microsoft Word documents and spreadsheets
- how to create custom reports with other data applications, that operate on the ODBC standard

User Guide

Online edition of the *User Guide*, which helps you learn how to use Network Discovery to accomplish tasks.

Reference Manual

Online edition of this manual.

Release Notes

Information about the most recent release of Network Discovery. Check here for information about late changes that do not appear in any of the manuals.

Icons

Displays all the device icons and package icons and says what they are.

Exceptions

Displays all the exceptions that Network Discovery tracks.

Supported Device and Port Attributes

Lists all attributes as displayed in the Device Manager and Port Manager. Attributes are also managed with the Attribute Manager.

Device Types

Table showing all device icons, their default priority, description, connectivity class and device class.

Device Filters

Lists all filters that can be applied to devices that have been discovered. Usually, a device that has been discovered but then filtered will not appear on the Network Map.

Device Title Filters

Lists all values for device titles that are filtered out when they appear in one or more of the MIB fields System Name, System Contact, System Location, and System Description.

Shortcuts

How to launch various aspects of Network Discovery directly from the URL field of your web browser.

About Network Discovery

Information about the makers of and modules within Network Discovery. Displayed at the top of the page is the Network Discovery version number.

Ways of opening Also available as a separate pull-down menu item from the Help button in the Health Panel or in any Network Map window.

Procedural Alert The help button in the top right hand corner of the About page leads to information about your browser.

Peregrine Systems Customer Support

A hyperlink to Peregrine Systems Customer Support Knowledge Base with answers to the questions most frequently asked about Network Discovery.

Close

Closes all Network Discovery windows except for the Toolbar and web browser-based windows.

Table 3: Windows closed by various commands

	File pull-down menu	Toolbar	
Windows	**Close Map**	**Close**	**Exit**
map windows	YES	YES	YES
Health Panel	—	YES	YES
Health Panel reports	—	YES	YES
Manager windows	—	YES	YES
Toolbar	—	—	YES

Exit

Quits Network Discovery, closing all windows except web browser-based windows.

Note: To completely exit Network Discovery, you must also exit your web browser.

Tip: If you close all web browser windows but leave the Toolbar open, you can re-open a web browser window by clicking any of the buttons in the second group (that is, Home, Status, Reports, Administration, or Help).

Tip: If you close the Toolbar window by clicking the window's close button, you can re-open the Toolbar by clicking any of the navigation hyperlinks in a web browser window except Status, Reports, Administration, or Help.

Procedural alerts

- If the Network Map is open and your map configuration has not been saved, you will be asked if you want to save your configuration.
- If you are not asked to save your configuration, you will be asked to confirm that you want to exit.

Navigating Network Discovery

Navigation Bar

At the bottom of the main browser windows (status, reports, administration, and help) are two rows of navigation hyperlinks called the Navigation Bar. These hyperlinks help you to visualize where you are in the menus, and help you navigate.

The first row shows where you are in the interface hierarchy. You can click items in the hierarchy to go up—all the way to the Home page, if you wish. Each part of the this row can be clicked except the right-most element.

The second row of hyperlinks represents the first and second groups of buttons from the Toolbar (Health Panel, Network Map, Events Browser, Service Analyzer, Find, Home, Status, Reports, Administration, and Help). Click any of these hyperlinks to navigate Network Discovery without using the Toolbar. If a hyperlink requires the Toolbar, it brings the Toolbar forward or opens it.

Menu Hyperlinks

In status, reports, administration, and help menus, you'll see small icons the left of each hyperlink. These icons classify the hyperlinks, and help you to identify them at a glance.

Table 4: Menu hyperlink icons

Icon	Hyperlink type
●	feature
🗀	folder
🗎	list, report, document
🗎	configuration
⚙	action
🗎	file export

CHAPTER 4

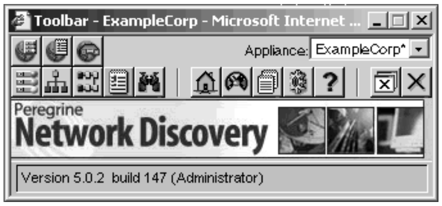
Aggregate Toolbar and Other Navigation

The Toolbar provides a way to navigate through Network Discovery. You may see one of two possible Toolbars:

Figure 4-1: Toolbars

If your Toolbar looks like this:

▶Consult this chapter.

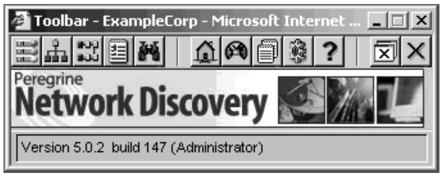

Toolbar - ExampleCorp - Microsoft Internet ...

Appliance: ExampleCorp

Version 5.0.2 build 147 (Administrator)

If your Toolbar looks like this:

▶See *Chapter 3, The Toolbar and Other Navigation*


Toolbar - ExampleCorp - Microsoft Internet ...

Version 5.0.2 build 147 (Administrator)

The main navigation buttons of the Toolbar are duplicated in the *Navigation Bar* on page 52, found at the bottom of many Network Discovery pages.

Important: This chapter is only of interest if you have multiple Peregrine appliances in your network, and if the Peregrine appliance you are using is in Aggregator mode.

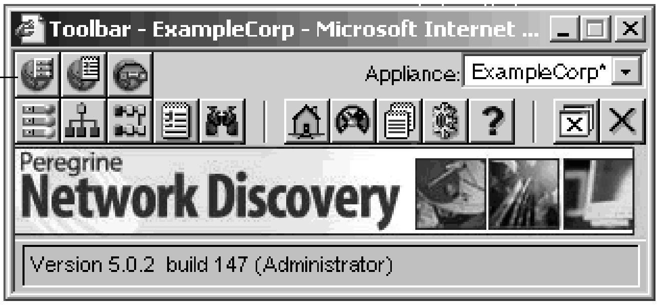
The Aggregator main Toolbar is similar to the single-appliance main Toolbar. Both allow you to navigate through Network Discovery.

The principal difference is that the Aggregator main Toolbar allows you examine all Peregrine appliances—the Aggregator appliance and all remote appliances—without logging in to each appliance separately.

Figure 4-2: The difference between an Aggregator Toolbar and a single-appliance

Toolbar is immediately visible: the Aggregator Toolbar has an extra row on top.

Figure 4-3: Aggregator Toolbar



An Aggregator Toolbar has an extra row of buttons

Toolbar - ExampleCorp - Microsoft Internet ...
Appliance: ExampleCorp*
Peregrine
Network Discovery
Version 5.0.2 build 147 (Administrator)

Here are the areas of an Aggregator Toolbar that are different:

- **Aggregate Health Panel** button
- **Aggregate Events Browser** button
- **Remote Appliances** button
- Appliance list
- **Home** button and Home Base page
- **Close** button
- **Exit** button

Note: All of the buttons in the second row affect only the active Peregrine appliance—that is, the appliance shown in the Appliance list—except for *Exit* on page 51.

The rest of the Aggregator Toolbar works exactly as the single-appliance Toolbar does. For more information about the Toolbar, see *Chapter 3, The Toolbar and Other Navigation*.

The first group of buttons controls Aggregator features:

Aggregate Health Panel	Opens the Aggregate Health Panel.	see *Aggregate Health Panel* on page 49, *Chapter 6, Aggregate Health Panel*, and *Chapter 7, Health Panel Menus*
Aggregate Events Browser	Opens the Aggregate Events Browser.	see *Aggregate Events Browser* on page 262
Remote Appliances	Lists the Peregrine appliances that can be viewed remotely and may be supplying data to the Aggregate Health Panel.	see *Remote Appliances* on page 49 and *Chapter 8, Remote Appliances*

Note: The first group of buttons always appears, even if the Aggregator has no remote appliances configured.

The second group of buttons contains the major functions of Network Discovery.

Health Panel	Opens the Health Panel.	see *Chapter 5, Health Panel*
Network Map	Open the Network Map window. (To have the Health Panel open automatically as well, see *Open Health Panel with Network Map* on page 93.)	see *Chapter 9, Network Map Window* and *Chapter 10, Network Map Menus*
Service Analyzer	View end-to-end network performance.	see *Chapter 15, Service Analyzer*
Events Browser	View recent events.	see *Chapter 16, Events Browser*
Find	Search for devices and ports of devices.	see *Chapter 17, Find*

The third group of buttons uses the active web browser window.

Home Base	The home page for the Aggregator appliance.	see *Home Base* on page 50 (also see *Home* on page 40)
Status	View configuration of the Peregrine appliance and of Network Discovery.	
Reports	View network statistics.	see *Chapter 18, Reports*
Administration	The function of this button depends on your account. ■ Demo users have no access to administration. ■ IT Employee users: Configure own account. ■ IT Manager: - Configure own account - Set appliance system variables ■ Administrator users: - Perform initial setup - Configure own and other accounts - Set appliance system variables - Set up Network Discovery	■ IT Employee and IT Manager users see *Chapter 19, Administration for IT Employee and IT Manager Accounts* ■ Administrator users see *Chapter 20, Administration for Administrator Accounts*
Help	Read documentation. This menu includes all manuals, release notes, and some quick-reference windows.	see *Help* on page 40

The fourth group of buttons controls your web browser environment.

☒	Close	Close all Network Discovery windows (except the Aggregate Health Panel and Aggregate Events Browser).	see *Close* on page 51 (also see *Close* on page 43)
✕	Exit	Quit Network Discovery completely, but leaves any active web browser windows open.	see *Exit* on page 51 (also see *Exit* on page 43)

Aggregate Health Panel

The Aggregate Health Panel is similar to the single-appliance Health Panel. The principal difference is that the Aggregate Health Panel presents the results of more than one Peregrine appliance.

The Aggregate Health Panel is discussed in detail in *Chapter 6, Aggregate Health Panel* and *Chapter 7, Health Panel Menus*.

Aggregate Events Browser

The Aggregate Events Browser is almost identical to the single-appliance Events Browser. The only visible difference is when a device is supplied from more than Peregrine appliance, it has a suffix "[via <Peregrine appliance name>]" for all appliances supplying the device.

Details of the Events Browser and Aggregate Events Browser are discussed in *Chapter 16, Events Browser*.

Remote Appliances

Remote appliances can be viewed without logging into each Peregrine appliance separately. Usually, remote appliances provide data for the Aggregator appliance—specifically, for the Aggregate Health Panel and the Aggregate Events Browser.

The Remote Appliances page is discussed in detail in *Chapter 8, Remote Appliances*.

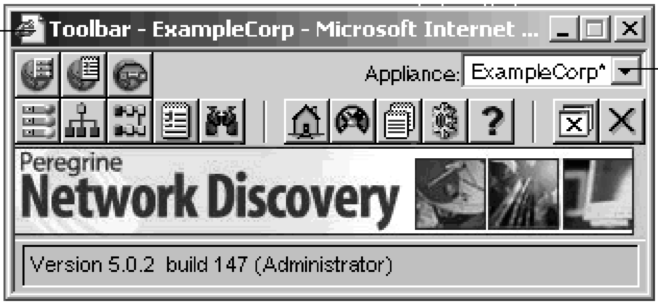
Appliance List

This pull-down list contains the Peregrine appliance that is acting as the Aggregator, and all the remote appliances.

The Aggregator appliance is listed at the top, using its system name—see *Appliance System Variables* on page 294. An asterisk appears after the system name to indicate that this is the Aggregator.

The appliance shown in this list affects what you see when you press a button in the second row. All of the buttons in the second row affect only the active Peregrine appliance. (The exception is the **Exit** button, since it closes all windows of all appliances, then closes the Toolbar itself.)

Figure 4-4: Aggregator Toolbar navigation



Appliance: ExampleCorp*

Version 5.0.2 build 147 (Administrator)

The banner shows what appliance you are working from. In this case you are working from the Aggregator

Shows what appliance you are looking at. The Aggregator is at the top of the list with an asterisk.

Limits

Only the first 20 characters of an appliance name are shown in this list. If the appliance name is longer than 20 characters, the first 18 characters are shown with a suffix of ".." to indicate the abbreviation of the name.

Related

To change the names shown in this list:

- To change a remote appliance name, see **Administration** > **Remote appliance administration** > **Remote appliance properties** (*Remote Appliance Properties* on page 327)
- To change the Aggregator appliance name, see *Appliance System Variables* on page 294.

Home Base

The Home button takes you to the Home Base page. The Home Base page is only available on an Aggregator appliance.

The menu on the Home Base page allows you to:

- open the Aggregate Health Panel
- select a remote appliance (also possible using the Appliance list in the Toolbar)
- perform operations on the Aggregator appliance without using the Toolbar

Close

Closes all Network Discovery windows for the Peregrine appliance shown in the *Appliance List* on page 50. Does not close the Aggregate Health Panel, the Aggregate Events Browser, the Toolbar, or web browser-based windows.

This is slightly different from the Close button in a single-appliance Toolbar, which closes everything except the Toolbar itself and web browser-based windows.

Table 1: Windows closed by various commands

	File pull-down menu	Toolbar	
Windows	**Close Map**	**Close**	**Exit**
map windows	YES	YES	YES
Health Panel	—	YES	YES
Aggregate Health Panel	—	—	YES
Health Panel reports	—	YES	YES
Aggregate Events Browser	—	—	YES
Manager windows	—	YES	YES
Toolbar	—	—	YES

Exit

The **Exit** button closes all windows of all appliances, then closes the Toolbar itself. Does not close web browser-based windows.

This is the only button in the second row that does not affect only the Peregrine appliance selected in the Appliance pull-down list. This button affects all appliance windows.

Navigation Bar

These hyperlinks behave in a way similar to that described in *Chapter 3, The Toolbar and Other Navigation*. However, there are important differences.

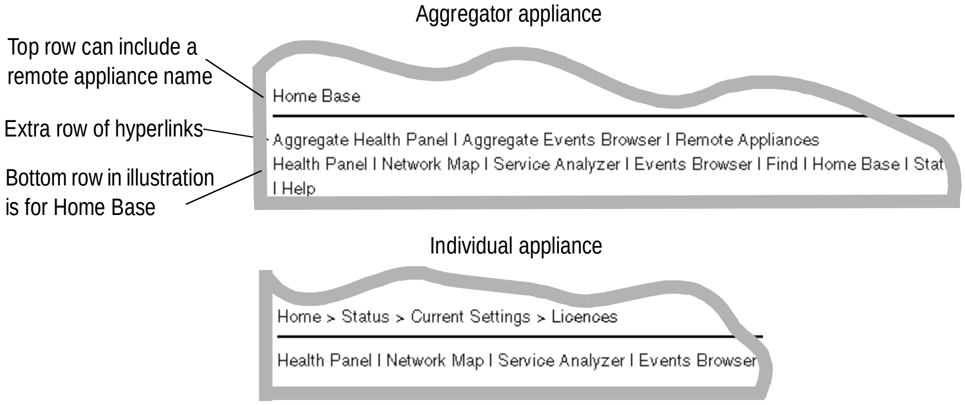
First, the top row can include a remote appliance name before the word “Home”, as in “nmAlgiers Home”.

Second, there is an extra row of hyperlinks. The extra (middle) row affects the Aggregator appliance. The new hyperlinks are “Aggregate Health Panel”, “Aggregate Events Browser”, and “Remote Appliances”.

Third, the bottom row of links can affect either the Aggregator appliance or a remote appliance.

- If the bottom row includes a “Home Base” hyperlink, clicking any of the links in this row affects the Aggregator appliance.
- If the bottom row includes a “Home” hyperlink, clicking any of the links in this row affects one of the remote appliances.

Figure 4-5: Differences in navigation bars


Aggregator appliance
Top row can include a remote appliance name
Extra row of hyperlinks
Bottom row in illustration is for Home Base
Home Base
Aggregate Health Panel | Aggregate Events Browser | Remote Appliances
Health Panel | Network Map | Service Analyzer | Events Browser | Find | Home Base | Stat
| Help
Individual appliance
Home > Status > Current Settings > Licences
Health Panel | Network Map | Service Analyzer | Events Browser

Important: The Toolbar and the navigation bar may affect different appliances.

Here is how the Appliance list can work in conjunction with the hyperlinks:

Scenario A

You begin with the Aggregator appliance, ExampleCorp, in the Appliance list.

1. From the Toolbar’s Appliance list, you select nmAlgiers.
2. You click the **Home** button.

   The Home page for nmAlgiers appears.
3. In the web browser window, you click the **Administration** hyperlink.

   The Administration menu for nmAlgiers appears.

In this scenario, the Appliance list and the navigation bar affect the same Peregrine appliance. However, this is not always the case.

Scenario B

You begin with a remote appliance, nmAlgiers, in the Appliance list.

1 From the Toolbar’s Appliance list, you select ExampleCorp.

2 You click the **Health Panel** button.

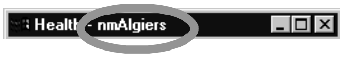
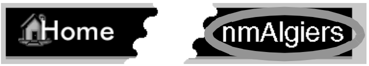
   The Health Panel for ExampleCorp appears.

3 In the web browser window, you click the **Status** hyperlink.

   The Status menu for nmAlgiers—*not* ExampleCorp—appears in the web browser window.

Note: Do not rely on the Appliance list in the Toolbar to determine the Peregrine appliance being affected. If you are using a remote appliance, its name is visible in a page banner.

Table 2: Visual cues to determine the active Peregrine appliance

If you click this button	The remote appliance name is visible	Example
Health Panel	in the banner of the new window	
Network Map		
Service Analyzer		
Events Browser		
Find		
Home	on the right side of the banner in the web browser window	
Administration		
Status		
Reports		
Help		

The remote appliance name also appears before the “Home” hyperlink in the first row of hyperlinks.

To select the appliance that the navigation bar relates to, you can:

- Choose the name in the Appliance list of the Toolbar, then click one of the middle section of buttons in the second row (Home, Administration, and so on). Under these circumstances, the hyperlinks open the Home page, the Administration page, and so on, of the device you chose in the Appliance list.
- Visit the Remote Appliances page, and click a remote appliance. You go to the Home page of the remote appliance.

CHAPTER 5 Health Panel

The Health Panel gives you an overview of the problems and potential problems in your network. You may see one or both of two Health Panels:

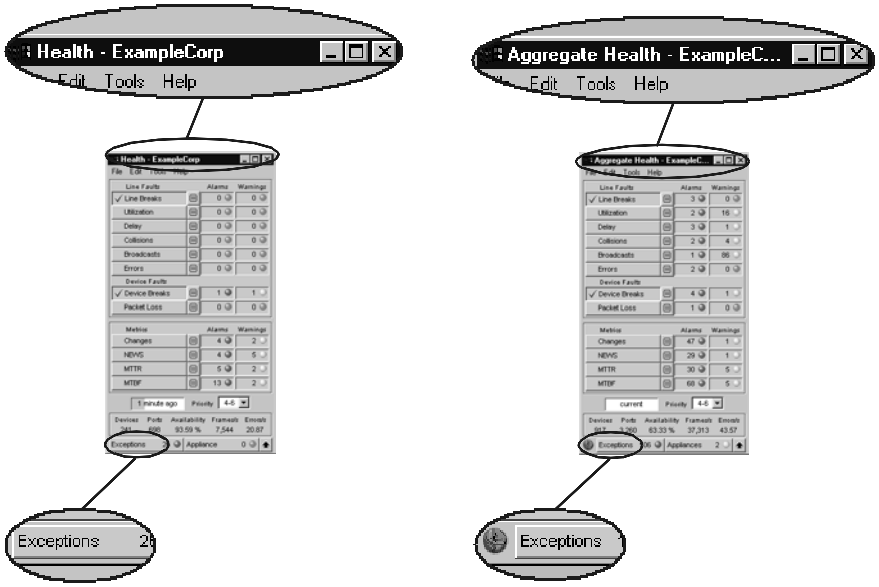
Figure 5-1: Different Health Panels

If the Health Panel looks like this:

▶Consult this chapter.

If the Health Panel looks like this:

▶See *Chapter 6, Aggregate Health Panel*.



- To explore buttons and controls on the Health Panel, see *Reports* on page 69 and:
  - *Line Breaks* on page 60
  - *Utilization* on page 60
  - *Delay* on page 61
  - *Collisions* on page 61
  - *Broadcasts* on page 61
  - *Errors* on page 62

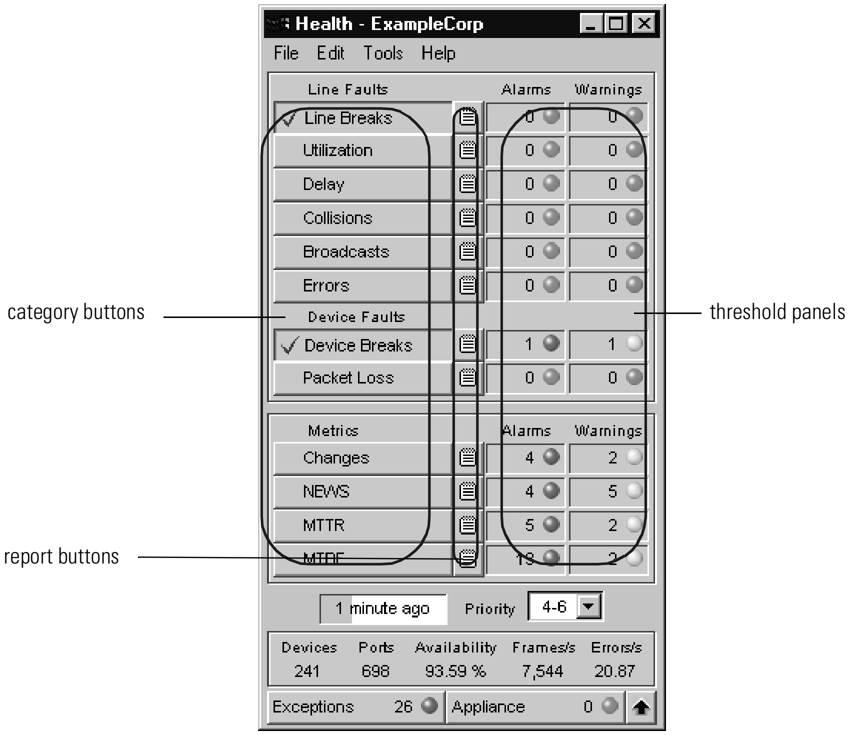
  - *Device Breaks* on page 62
  - *Packet Loss* on page 64
  - *Changes* on page 65
  - *NEWS* on page 68
  - *MTTR* on page 68
  - *MTBF* on page 69
- To interpret the statistics reported on the Health Panel or to learn about the Exceptions button or the Appliance button, see *Other Controls and Displays* on page 72.
- To explore commands in pull-down menus, see *Chapter 7, Health Panel Menus*.

Introduction

The Health Panel gives you an overview of the problems and potential problems in your network.

The Health Panel can be used alone or in conjunction with the Network Map. Used by itself, the Network Map gives you an overview of the topology of your network. Used with the Health Panel, the Network Map helps you to understand the cause of problems and their effects.

Figure 5-2: Health Panel (detailed view)



Line Faults	Alarms	Warnings
✓ Line Breaks	0	0
Utilization	0	0
Delay	0	0
Collisions	0	0
Broadcasts	0	0
Errors	0	0
Device Faults		
✓ Device Breaks	1	1
Packet Loss	0	0

Metrics	Alarms	Warnings
Changes	4	2
NEWS	4	5
MTTR	5	2
MTBF	13	2

1 minute ago   Priority 4-6

Devices	Ports	Availability	Frames/s	Errors/s
241	698	93.59 %	7,544	20.87

Exceptions 26   Appliance 0

The default view of the Health Panel shows all fault and metric categories. Each category has a category button, a report button, and a threshold panel.

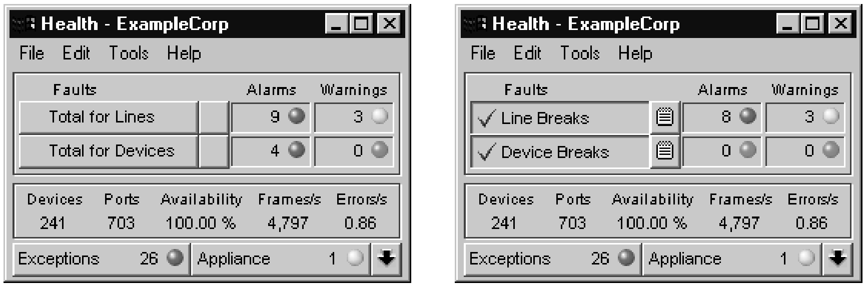
The threshold panel is divided in two halves, one each for alarms and warnings. Each half shows a number and a signal light. The number represents the number of lines or devices that have crossed a threshold, and the color of the signal lights show the threshold that has been crossed. If a category has no faults, both halves of the threshold panel will show 0 and an OK signal light.

Note: For the first 24 hours that Network Discovery ™ is in operation, Device Breaks will show warnings only—no alarms. Network Discovery does not report alarms during this period to allow diagnostic probabilities to become stable. Similarly, devices that have been discovered within the past 24 hours will not contribute to the alarms Device Breaks total.

The Health Panel has two ways to display the details of each category: graphic and textual. Graphic results are shown in map windows—see *View* on page 150. Textual results appear in text windows called Health Panel reports—see *Reports* on page 69.

The detailed view of the Health Panel shows all the problems for all categories. This gives an overview of the network. There are two other views—the brief totals view and the brief focus view.

Figure 5-3: Health Panel (brief views)



Health - ExampleCorp

Faults	Alarms	Warnings
Total for Lines	9 ●	3 ○
Total for Devices	4 ●	0 ●

Devices	Ports	Availability	Frames/s	Errors/s
241	703	100.00 %	4,797	0.86

Exceptions 26 ● Appliance 1 ○

Health - ExampleCorp

Faults	Alarms	Warnings
✓ Line Breaks	8 ●	3 ○
✓ Device Breaks	0 ●	0 ●

Devices	Ports	Availability	Frames/s	Errors/s
241	703	100.00 %	4,797	0.86

Exceptions 26 ● Appliance 1 ○

The brief totals view shows the total alarms and total warnings for all fault categories. (Metric categories are not included.) The brief focus view shows only the selected category buttons. Both brief views are intended for use with map windows. Once in a brief view, click the category buttons to switch to the other brief view.

To switch between summary view and one of the brief views, see *Switch view* on page 74.

Note: Event notification is not handled by the Health Panel. Event notification is handled by filters created by the Network Discovery Administrator or another Administrator account. See *Event Filter Configuration* on page 337.

Limits

Most limits on the Health Panel depend on whether it is used alone or in conjunction with a Network Map.

Table 1: Basic restrictions on the Health Panel

Limit	Health Panel only	Health Panel with Network Map
Number of concurrent Health Panels	250 (same as number of accounts)	depends on how many map session licenses the Peregrine appliance has
Data refresh rate	depends on all sampling periods of all remote appliances, but checked every 60 seconds	depends on sampling period of the Peregrine appliance

Default

Default colors for signal lights are:

- *alarm color:* red
- *warning color:* yellow
- *OK color:* green

Fault Category Buttons

Check marks indicate the selected button or buttons.

Up to two buttons can be selected at a time: one for Line Faults and one for Device Faults. Selecting a Metrics button will deselect any selected Fault buttons.

Effects

Selected buttons have effects on map windows:

- Line Faults buttons: lines will be drawn in colors that indicate their alarm state
- Device Faults buttons: icons will have colored rings that indicate their alarm state
- Metrics buttons: icons will have colored rings that indicate their alarm state

Whether devices have colored rings depends on priority. If the priority assigned to the device is equal or greater than the priority view for the Health Panel, a device will have a ring. All devices of lower priority will have no ring.

The selected buttons will also appear in the *Status Bar* on page 107, of a map window.

If you have a map open

▶ The selected button will immediately have an effect (described above) on the map window.

If you do not have a map open

1. A dialog asks if you want to open a map session.
2. Click **Yes**.

The selected button will have an effect (described above) on the map window.

Default

- *Line Fault:* Line Breaks
- *Device Fault:* Device Breaks

Related

To change whether a device is affected by fault category buttons, see *Properties* on page 159, or *Priority List* on page 72.

Recorded Faults

Recorded faults are divided into line faults and device faults.

All faults that occur are based on the *Alarm Thresholds…* on page 142, as set by the Network Discovery Administrator or other Administrator account.

Whether a fault is visible to a given account depends on the priority range for the account—see *Priority List* on page 72—and the priority of devices and lines for the current map configuration—see *Properties* on page 159 and *Priority* on page 28.

Line Faults

Line faults include:

- Line Breaks
- Utilization
- Delay
- Collisions
- Broadcasts
- Errors

Note: No alarmed (or warned) lines will appear on the Network Map if all alarmed (or warned) lines are within packages. Line faults do not affect the color of rings around packages.

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. Although both input and output are considered to be broken, only the input port is alarmed.

Default Selected

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.

Default Depends on the alarm type for the interface, but typical values are:

- *alarm*: 85% of available bandwidth
- *warning*: 65% of available bandwidth

Delay

Identifies 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. Includes only the time a packet waits in the router queue before being transmitted plus the time to process the packet at the other end after being received. Does not include the delay across the link.

Frequently caused by

Overloaded device buffers

Default

- *alarm:* 2 milliseconds
- *warning:* 1 millisecond

Collisions

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

Frequently caused by

Too many devices connected to a segment

Technical

MIB object dot3StatsEntry (where supported by device); Ethernet half-duplex only

Default

- *alarm:* 100 collisions per second
- *warning:* 50 collisions per second

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 is no warning threshold for broadcasts. Instead, the alarm and warning colors are used to identify lines that are the source of broadcasts (alarm color) and lines that are carrying broadcasts (warning color).

Default

50 frames per second

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.

Frequently caused by

- faulty device
- wiring problem

Default

- *alarm:* 2 frames per second
- *warning:* 1 frame per second

Device Faults

Device faults include:

- Device Breaks
- Packet Loss

Device Breaks

Diagnoses break faults on real network devices (not scanned-only devices), whether SNMP managed or not. Determines if a device is not responding or transmitting.

Network Discovery defines a break as continued failure after a minimum number of attempts at contact, lasting at least 90 seconds.

Causes of loss of SNMP contact

- Network causes
    - the device is physically broken
    - the device has been turned off
    - the device’s SNMP management has failed
    - the device is working but seems not to be responding because the line is broken
    - the device is being masked by another device with a break alarm
    - recent SNMP packets to or from the device have been lost or corrupted
- Administrative causes
    - the device’s community string has been changed to a string that Network Discovery does not know

Effects

If Network Discovery determines that a device is broken, it does not assume that all devices beneath it are broken and identify them with break alarms. Instead, Network Discovery identifies each such device with a break warning, signifying that data is not available from the device and that the device could be broken.

Once the broken device is fixed, break warnings will disappear if Network Discovery was merely out of contact with the device.

Options

There are two types of break fault diagnosis, fast and normal.

Table 2: Time and availability of break fault diagnosis

Mode	Alarm time	Warning time	Available to devices
fast	2 minutes	n/a	■ with IP addresses *and* ■ with a priority of 3 (or higher) *and* ■ that respond to pings *and* ■ that are accessible to the Peregrine appliance through a LAN link
normal	3–6 minutes*	<3 minutes	all other devices

* A typical value for managed devices in a network with 3,000 devices.

In normal mode, the time to generate an alarm depends on several factors:

Table 3: Factors affecting time to generate break alarm (normal mode)

Origin	Factor
Major	
network	length of sampling period
device	current and recent SNMP drop rate
device	location
device	SNMP management
device	number of ports
Minor	
nearby devices	SNMP drop rate

Unmanaged workstations with no IP address take the longest to diagnose.

Limits

There are no thresholds for breaks, since a device is either broken or it is not.

Break alarms indicate a 99.5% certainty that a device is broken, and take some time to appear. Break warnings give more rapid alerts of possible break faults.

Note: For the first 24 hours that Network Discovery is in operation on your network, Device Breaks will show 0 faults. Network Discovery does not report breaks during this period to allow diagnostic probabilities to become stable.

Also, for the first 24 hours after a device is first discovered by Network Discovery, Device Breaks for this device will not be diagnosed. Again, this lets the diagnostic probabilities stabilize.

Default

Selected

Related

Time to diagnose a break is reported in the Device Manager's *Diagnosis* on page 192, panel.

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.

Frequently caused by

An overloaded device or connection

Limits

Available only when unicast data is available for all ports.

Technical

(sum (in_unicasts) - sum (out_unicasts)) / sum (in_unicasts)

Default

- *alarm:* 25%
- *warning:* 10%

Metrics

Metrics include:

- Changes
- NEWS
- MTTR
- MTBF

Changes

Identifies devices recently added, devices that have recently moved (or more precisely, had a connection changed) and devices not recently seen.

Table 4: Alarm states for Changes

State	Meaning
alarm	■ device has been added ■ device has been moved
warning	device has not been seen (and may be trashed soon)

In all cases, the term “recently” reflects the Changes setting in *Alarm Thresholds…* on page 142.

Note: Once Network Discovery has not had contact with a device for a period greater than the threshold (by default, 6 hours), it will be displayed with a red ring. Once the “not seen” period has exceeded 24 hours, the device will also be displayed with a gray circular background. (This does not apply to scanned-only devices.)

Table 5: Speed of detection of connection changes

Type	Time to determine (average)
traffic-based	1 hour—several days
table-based	3 hours
source address capture	3 minutes—1 hour

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

The Health Panel summarizes connectivity changes to the network. Each device should contribute only a single alarm or warning. (If there is more than one alarm or warning per device or per port, they will be displayed in the Device Manager or Port Manager.)

Adds

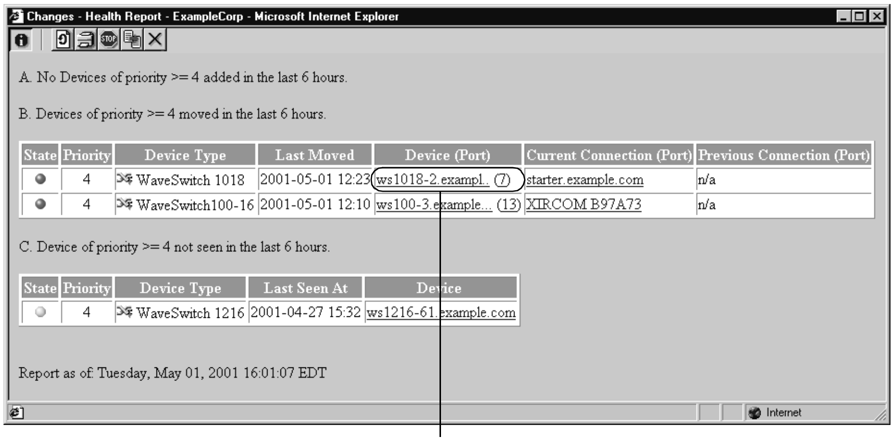
Adds are devices recently added to the map. (An added device may or may not be recently discovered.)

Moves

Moves are devices that have recently had a connection changed.

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

Figure 5-4: Changes report



Changes - Health Report - ExampleCorp - Microsoft Internet Explorer

A. No Devices of priority >= 4 added in the last 6 hours.

B. Devices of priority >= 4 moved in the last 6 hours.

State	Priority	Device Type	Last Moved	Device (Port)	Current Connection (Port)	Previous Connection (Port)
●	4	WaveSwitch 1018	2001-05-01 12:23	ws1018-2.exampl.. (7)	starter.example.com	n/a
●	4	WaveSwitch100-16	2001-05-01 12:10	ws100-3.example... (13)	XIRCOM B97A73	n/a

C. Device of priority >= 4 not seen in the last 6 hours.

State	Priority	Device Type	Last Seen At	Device
○	4	WaveSwitch 1216	2001-04-27 15:32	ws1216-61.example.com

Report as of: Tuesday, May 01, 2001 16:01:07 EDT

anchor device

For recently moved devices, the higher priority device is considered to be the anchor, or the device to which the change has happened. (The higher priority device is usually a network connectivity device, such as a router or switch.) The connection is associated primarily with the connection on the anchor device, not the device that moved.

Table 6: Moved device data

Category	Column	Contents
Device	Priority	priority of the anchor device
	Type	■ icon ■ icon type
	Title (Port)	■ title ■ port—optional
Last Changed At	When	date and time
	Graphic	■ ✚ connection has appeared on this device ■ ▬ connection has disappeared on this device ■ ☾ connection has moved on this device
Previous / Current Connection	Via	always a virtual device (or blank)
	Type	■ icon ■ icon type
	Title (Port)	■ title ■ port—optional

Example: A workstation is attached to a switch at port 2. You detach the workstation from port 2, and reattach it to port 8. The change is recorded on the switch, not the workstation.

Not Seen

"Not seen" devices are those with which Network Discovery has lost contact and which may soon disappear from the Network Map.

Limits

Device Added

- Does not include virtual devices

Device Moved

- Does not include virtual devices as anchor devices—connections to a virtual device are not considered relevant
- Does not include cases where the current and previous connections are to virtual devices
- Does not include added ports
- 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).

Device Not Seen

- Does not include virtual devices

When to use it

- To detect the adding of unauthorized devices to your network.
- To detect the unauthorized moving of devices within your network.
- To concentrate on changes for a specific time period.

Example: On Monday morning, you discover several problems that were not present on Friday at quitting time.

To view specific changes

1. Set the Changes threshold to 64 hours—see *Alarm Thresholds…* on page 142.
2. Set the Health Panel priority to 1–6.
   - Devices that have been added to the network (within the past 64 hours) will now be highlighted with an alarm ring.
   - Devices that have been moved within the network (within the past 64 hours) will be now be highlighted with an alarm ring.
   - Devices with which Network Discovery has lost contact for *all* of the past 64 hours, and which may soon be removed from the network, will be highlighted with a warning ring.

Effects

When Network Discovery determines that a connection first exists, and when Network Discovery determines that a connection no longer exists, it sets the "time of last change" to the current time.

If a device is connected to a port on a hub, then disconnected, and a new device is connected to the same port on the hub, Network Discovery will record three change alarms: one for the hub, one for the original device, and one for the new device.

Disconnecting a device and then reconnecting it to the same port will not create a new "time of last change"; neither will turning a device on and off. (Unless the device is disconnected or turned off for so long that the device is removed from the Network Map.)

Default 6 hours

NEWS

Network Early Warning System (NEWS) predicts which devices will soon have an alarm or warning for packet loss or utilization, whichever will come first for a given device. Monitors the changing levels for both factors and determines how rapidly each is changing. Uses the peak busy minute per week for both values.

NEWS reports its prediction in days.

A "days until" value of 0 means:

- the object has already crossed the threshold
- Network Discovery predicts that the object will repeatedly cross the threshold from now on

Assumes that the network does not change—that is, that no devices are added or removed, and that lines are not altered.

Default

- *alarm:* 180 days
- *warning:* 365 days

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.

Default

- *alarm:* 48 hours
- *warning:* 24 hours

Related Administrator: To reset MTTR for a device, see *Reset MTTR and MTBF [Administrator or IT Manager only]* on page 162.

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 Network Discovery has seen it fail twice. The MTBF for this device is 50 days.

Default

- *alarm:* 180 days
- *warning:* 365 days

Related

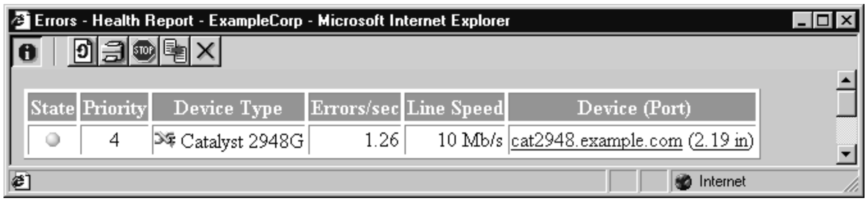
Administrator: To reset MTBF for a device, see *Reset MTTR and MTBF [Administrator or IT Manager only]* on page 162.

Reports

Health Panel reports list all devices or ports that have crossed an alarm or warning threshold.

All reports provide one row of data for each alarm or warning.

Figure 5-5: Sample Health Panel report


Errors - Health Report - ExampleCorp - Microsoft Internet Explorer
Internet

State	Priority	Device Type	Errors/sec	Line Speed	Device (Port)
○	4	Catalyst 2948G	1.26	10 Mb/s	cat2948.example.com (2.19 in)

The rows are sorted by state, by priority, by value, and alphabetically by device title. The rows of a Line Faults report have two extra columns for data not meaningful in a Device Faults report.

Table 7: Data reported in a Health Panel report

Column	Line	Device	Notes*
State	YES	YES	alarm | warning
Priority	YES	YES	1–6
Device Type	YES	YES	—
Value	YES	YES	see Table 8 on page 70
Line speed	YES	—	in Gb/sec., Mb/sec., kb/s, or b/s
Device	YES	YES	hyperlinked to Device Manager
Port	YES	—	hyperlinked to Port Manager

* The Changes report does not follow this model.

Table 8: Values for a Health Panel report

Category	Value
Line Breaks	Broken since (time/date)
Utilization	Utilization (%)
Delay	Response time (milliseconds)
Collisions	Collisions/sec.
Broadcasts	Frames/sec.
Errors	Frames/sec.
Device Breaks	Broken since (time/date)
Packet Loss	Unicasts formula (%)
NEWS	Days until
MTTR	MTTR (hours)
MTBF	MTBF (days)

When to use it

- If you prefer tabular data over a visual representation.
- When you want to have a static display of faults at a given moment.

Limits

- No faults below the Priority range will be displayed
- Reports are updated every poll cycle. The Device Breaks report can be updated more frequently when fast break detection applies (see *Device Breaks* on page 62).

Related

These reports are also available from the **Tools** pull-down menu of the Health Panel or any map window—see *Health Panel Reports* on page 166.

Each Health Panel report has a toolbar:

About

Displays the Health Panel report.

Refresh

Refreshes the contents of the Health Panel report.

Print

Sends the contents of the Health Panel report to a printer attached to the management workstation.

Text

Displays the contents of the Health Panel report as text that can be copied and pasted.

Note: May cause the report to be refreshed with new data.

Procedural alert

To return to non-text mode, click **About** again.

Close

Closes the window and exits the Health Panel report.

Other Controls and Displays

Progress Bar

The color of the bar indicates:

- when the Health Panel was last refreshed (gray portion, on the left)
- when the Health Panel will be refreshed again (white portion, on the right)

The elapsed time since the last refresh is superimposed on the progress bar.

When a map is open and *Forecast* on page 168, is being used, the entire bar will be gray and the text will indicate the prediction period.

Note: Also displayed in status bar of a map window.

Note: Fast breaks can occur at any time, but do not affect the progress bar.

Limits If the Network Mapper has not yet mapped any devices, the progress bar is static.

Priority List

Establishes the minimum priority that will generate an alarm or warning.

This priority is compared against the device/line priorities defined by the user's account. This is the case (even if you open a Health Panel on a remote appliance from an Aggregator appliance).

Effects

- Affects all your map configurations.
- Any device or line with a priority less than the minimum priority:
  - will not generate an alarm or warning on the Health Panel
  - will not contribute to the alarm or warning counts on the Health Panel

For information on default priorities, see *Priority* on page 28.

Note: Devices and lines that are below your minimum priority may still generate an alarm in the Events Browser or an event notification (e-mail or page), since event filters for those areas are based on the Prime configuration.

Limits 1–6

Default 3 (shown as “3-6”)

Statistics

These five statistics reflect the state of the entire network as viewed by Network Discovery.

Devices

The number of mapped devices. Also displayed in the Network Map window's status bar. A display of your mapped devices and discovered devices can be found in the **Status** menu's **Appliance Health** report, where they are compared against your licenses.

Ports

The number of mapped ports. A display of your mapped ports and discovered ports can be found in the **Status** menu's **Appliance Health** report, where they are compared against your licenses.

Availability

This percentage is obtained by dividing the number of operational devices by the total number of devices in the network. Only devices with priorities 3–6 are used in the calculation. Scanned-only devices are not used in the calculation.

Frames/s

Represents the instantaneous number of frames per second seen on the entire network.

Errors/s

Represents the instantaneous number of errors per second seen on the entire network. Includes errors from both in and out ports.

Special buttons

The two buttons with labels at the bottom of the Health Panel, **Exceptions** and **Appliance**, indicate whether Network Discovery is having problems mapping your network. The indicators for these two buttons will alert you if Network Discovery is running into difficulties.

There are two types of problem that can cause Network Discovery to experience problems in mapping a network:

- "standards" problems with devices in the network, tracked by **Exceptions**
- problems with the Peregrine appliance, tracked by **Appliance**

The signal lights for these two buttons work slightly differently from the other signal lights on the Health Panel. Instead of two lights, one each for alarms and warnings, there is one light that reports the most critical state. If there are both alarms and warnings, the signal light will indicate an alarm. If there are only warnings, the signal light will indicate a warning.

The numbers for these buttons indicate the total number of alarm and warnings.

When you click one of these special buttons, you will be taken to a report (also available from the Reports menu).

Exceptions

Exceptions indicate problems with your network that the Network Discovery Administrator should address—for example, an incorrect netmask or a non-standard SNMP MIB. Exceptions prevent Network Discovery from accurately discovering and mapping your network.

Includes the total number of exceptions that produce alarms and warnings. Does not include informative exceptions.

Related See also **Reports** > **Support Reports** (*Support Reports* on page 276).

Appliance

Takes you to **Status** > **Appliance Health**. Indicates problems with your Peregrine appliance that your Peregrine Systems Customer Support representative will help you address.

Appliance Health indicates the health both of the major subsystems that make up the Network Discovery software (such as the Explorer, Interrogator, Pollers, and Mapper) and the operating environment of the Network Discovery appliance (such as hard disk drive space and CPU load). If there are permanent problems or persistent transient problems, report them to Peregrine Customer Support.

Related See also **Status** > **Appliance Health**.

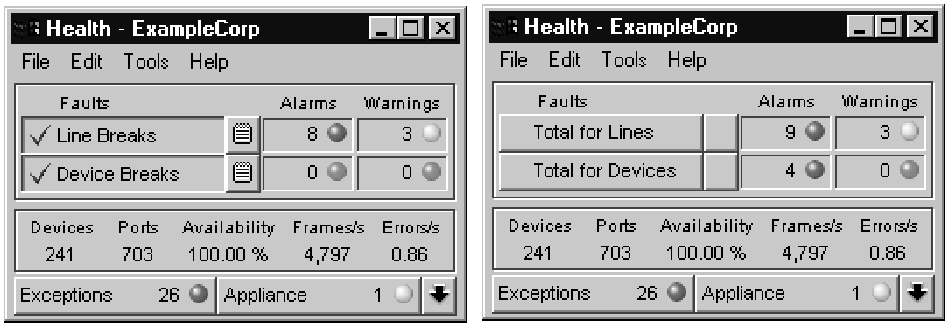
⬆ ⬇ Switch view

The Health Panel has two different views, detailed and brief.

The brief view can serve two purposes: it can display the total alarms and warnings for all line faults and device faults, or it can focus on the selected fault category buttons.

When you are displaying the totals, clicking a fault category button will change the button to the button you had selected in the detailed view. If no button is selected in the detailed view, the buttons will change to Line Breaks or Device Breaks.

Figure 5-6: Health Panel—brief views



Faults	Alarms	Warnings
✓ Line Breaks	8 ●	3 ○
✓ Device Breaks	0 ●	0 ●

Devices	Ports	Availability	Frames/s	Errors/s
241	703	100.00 %	4,797	0.86

Exceptions 26 ● Appliance 1 ○ ⬇

brief view with focus on selected categories

Faults	Alarms	Warnings
Total for Lines	9 ●	3 ○
Total for Devices	4 ●	0 ●

Devices	Ports	Availability	Frames/s	Errors/s
241	703	100.00 %	4,797	0.86

Exceptions 26 ● Appliance 1 ○ ⬇

brief view with totals

When to use detailed view

- when you want a detailed overview of current faults in your network
- when selecting fault category buttons

When to use brief views

- when you want a summary of current faults in your network (totals view)
- when you want to focus on selected fault category buttons and their effects on map windows (focus view)
- whenever you want to minimize the size of the Health Panel (either view)

Related

To start up with a brief view, see *Use brief Health Panel* on page 147.

6 CHAPTER Aggregate Health Panel

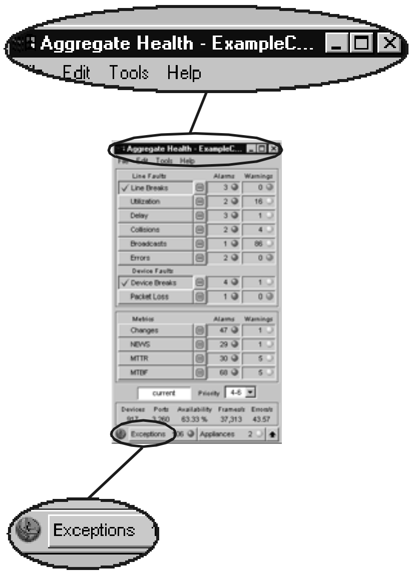
Important: This chapter is only of interest if you have multiple Peregrine appliances in your network, and if the Peregrine appliance you are using has an Aggregator license.

The Health Panel gives you an overview of the problems and potential problems in your network. You may see one or both of two Health Panels:

Figure 6-1: Different Health Panels

If the Health Panel looks like this:

▶Consult this chapter.



Line Faults		Alarms	Warnings
✓ Line Breaks	⊟	3 ●	0 ●
Utilization	⊟	2 ●	16 ○
Delay	⊟	3 ●	1 ○
Collisions	⊟	2 ●	4 ○
Broadcasts	⊟	1 ●	86 ○
Errors	⊟	2 ●	0 ●
Device Faults			
✓ Device Breaks	⊟	4 ●	1 ○
Packet Loss	⊟	1 ●	0 ●

Metrics		Alarms	Warnings
Changes	⊟	47 ●	1 ○
NEWS	⊟	29 ●	1 ○
MTTR	⊟	30 ●	5 ○
MTBF	⊟	68 ●	5 ○

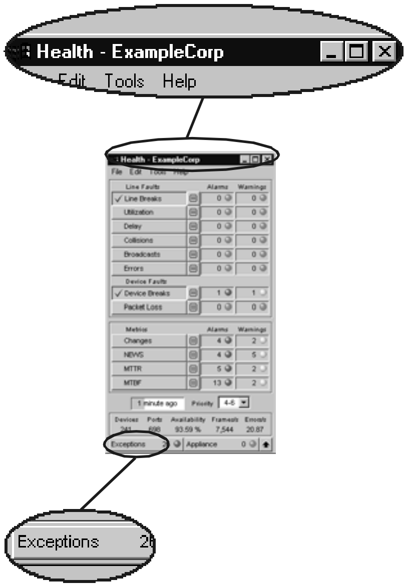
current Priority 4-6

Devices	Ports	Availability	Frames/s	Errors/s
[illegible]	3,260	63.33 %	37,313	43.57

Exceptions 306 ● Appliances 2 ○

If the Health Panel looks like this:

▶See *Chapter 5, Health Panel.*



Line Faults		Alarms	Warnings
✓ Line Breaks	⊟	0 ●	0 ●
Utilization	⊟	0 ●	0 ●
Delay	⊟	0 ●	0 ●
Collisions	⊟	0 ●	0 ●
Broadcasts	⊟	0 ●	0 ●
Errors	⊟	0 ●	0 ●
Device Faults			
✓ Device Breaks	⊟	1 ●	1 ○
Packet Loss	⊟	0 ●	0 ●

Metrics		Alarms	Warnings
Changes	⊟	4 ●	2 ○
NEWS	⊟	4 ●	5 ○
MTTR	⊟	5 ●	2 ○
MTBF	⊟	13 ●	2 ○

1 minute ago Priority 4-6

Devices	Ports	Availability	Frames/s	Errors/s
241	698	93.59 %	7,544	20.87

Exceptions 26 ● Appliance 0 ●

The Aggregate Health Panel is similar to the single-appliance Health Panel. The principal difference is that the Aggregate Health Panel presents the results of more than one Peregrine appliance.

Here are the areas of the Aggregate Health Panel that are most different:

- *Appearance* on page 79
- *Threshold Panels* on page 79
- *Category Buttons* on page 79
- *Aggregate Health Panel Reports* on page 80
- *Progress Bar* on page 80
- *Statistics* on page 81
- *Exceptions Button* on page 82
- *Appliances Button* on page 82
- *Pull-down Menus* on page 83

There is one area with a similarity that is easy to overlook:

- *Priority List* on page 81

Appearance

- The panel’s banner reads “Aggregate Health Panel” rather than “Health Panel”.
- There is a small globe icon in the bottom left corner of the Aggregate Health Panel.

Threshold Panels

The threshold panels are composed of numbers and signal lights in two columns, alarms and warnings. The number represents the number of lines or devices that have crossed a threshold, and the color of the signal lights show the threshold that has been crossed.

The numbers and signal lights in the alarms and warnings columns represent totals from multiple Peregrine appliances—from all functional remote appliances, and from the Aggregator appliance.

Related The threshold panels of the single-appliance Health Panel are discussed in *Introduction* on page 57.

Category Buttons

In the single-appliance Health Panel, the category buttons serve to highlight specific conditions in the associated map window. There is no single map window associated with the Aggregate Health Panel, so the category buttons apply to all open Network Maps. Any buttons that you select on the Aggregate Health Panel will also be selected on single-appliance Health Panels.

If you switch to brief view with categories selected, the selected categories also appear in the brief view.

Related The category buttons of the single-appliance Health Panel are discussed in *Fault Category Buttons* on page 59.

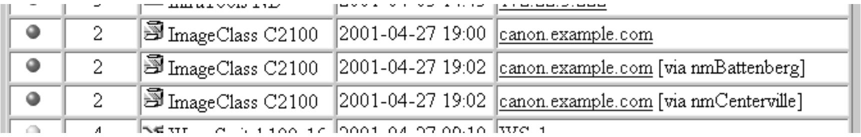
Aggregate Health Panel Reports

Health Panel reports list all devices or ports that have crossed an alarm or warning threshold.

The devices and ports listed in the Health Panel reports are from multiple Peregrine appliances—from all functional remote appliances, and (optionally) from the Aggregator appliance.

The same device can appear multiple times in this list. Whether or not a device appears multiple times depends entirely on the address scope defined for each individual Peregrine appliance.

Figure 6-2: Sample of multiple instances of a device



●	2	ImageClass C2100	2001-04-27 19:00	canon.example.com
●	2	ImageClass C2100	2001-04-27 19:02	canon.example.com [via nmBattenberg]
●	2	ImageClass C2100	2001-04-27 19:02	canon.example.com [via nmCenterville]

When a device is from a remote appliance, it has a suffix “[via <remote appliance name>]”. When a device is from the address scope of the Aggregator itself, it has no suffix.

The report banner reads “Aggregate Health Panel” rather than “Health Panel”.

Related

- The reports of the single-appliance Health Panel are discussed in *Reports* on page 69.
- To set a remote appliance name, or to add a remote appliance, see *Remote Appliance Administration* on page 327.

Progress Bar

The position of the bar indicates both when the data to the Aggregate Health Panel was last refreshed (gray portion), and when it will be refreshed again (white portion).

The Aggregate Health Panel is refreshed every 60 seconds, whereas the refresh rate of the single-appliance Health Panel depends on the poll cycle for that Peregrine appliance. Data is updated when the poll cycle completes on any Peregrine appliance.

Note: Fast breaks can occur at any time, but do not affect the progress bar.

Related

The progress bar of the single-appliance Health Panel is discussed in *Progress Bar* on page 72.

Priority List

Establishes the minimum priority that will generate an alarm or warning.

This priority is compared against the device/line priorities defined by Prime (for the Aggregator appliance). This is true even if the Aggregator appliance is aggregating only itself—that is, for any device that has an Aggregator license but which has no remote appliances defined as data sources.

Effects

- Affects all your map configurations.
- Any device or line with a priority less than the minimum priority
  - will not generate an alarm or warning on the Health Panel
  - will not contribute to the alarm or warning counts on the Health Panel

Procedural alerts

When you set the priority in the Aggregate Health Panel, you also set the priority in all single-appliance Health Panels. (The reverse is also true.)

Related

The priority list of the single-appliance Health Panel is discussed in *Priority List* on page 72.

Statistics

These five statistics reflect the state of all Peregrine appliances.

Table 1: Statistics

Statistic	Explanation
Devices	The number of mapped devices.
Ports	The number of mapped ports.
Availability	The number of operational devices (of priority 3 or higher) divided by the total number of devices (of priority 3 or higher).
Frames/s	The instantaneous number of frames per second seen.
Errors/s	The instantaneous number of errors per second seen.

Important: There can be duplicate devices. The Aggregator does not eliminate duplicates. If you have included a device in the discovery ranges for more than one remote appliance, the Aggregator treats each occurrence as a unique device and reports statistics for all of them.

Related

The statistics of the single-appliance Health Panel are discussed in *Statistics* on page 73.

Exceptions Button

Exceptions are problems with your network that the Network Discovery Administratorshould address—for example, an incorrect netmask or a non-standard MIB. Exceptions prevent Network Discovery from accurately discovering and mapping your network.

This button reports the total number of exceptions for all Peregrine appliance (Aggregator and remote appliances).

Instead of dual signal lights and dual numbers as used on the threshold panel, this button has:

- a single signal light that reports the most critical state
- a single number that indicates the total number of alarms and warnings.

When you click this button, you are taken to a report (also available from the Status menu).

Related The Exceptions button of the single-appliance Health Panel is discussed in *Exceptions* on page 74.

Appliances Button

Takes you to **Status** > **Appliance Health**. Indicates problems with your Peregrine appliance that your Peregrine Systems Customer Support representative will help you address.

Appliance Health indicates the health both of the major subsystems that make up the Network Discovery software (such as the Explorer, Interrogator, Pollers, and Mapper) and the operating environment of the Network Discovery appliance (such as hard disk drive space and CPU load). If there are permanent problems or persistent transient problems, report them to Peregrine Customer Support.

This button informs you if the Aggregator has problems receiving data from a remote appliance or if there are problems with the remote appliance itself. Typical problems include:

- data from a remote appliance is stale or outdated
- inability to connect to a remote appliance (for example, the Aggregator cannot receive data because the remote appliance is configured incorrectly)
- unavailability of a remote appliance (for example, the remote appliance is not working, and no device can contact it)

If a remote appliance is not available, the Aggregator uses the last available imported Health Panel for that remote appliance.

Instead of dual signal lights and dual numbers as used on the threshold panel, this button has:

- a single signal light that reports the most critical state
- a single number that indicates the total number of alarms and warnings.

Related The similar Appliance button of the single-appliance Health Panel is discussed in *Appliance* on page 74.

See also **Status** > **Appliance Health**.

Pull-down Menus

Some commands in the pull-down menus of the Aggregate Health Panel will be disabled (and therefore dimmed).

Table 2: Disabled pull-down commands

Menu	Command	Associated with
Edit	Alarm Thresholds	map window
Tools	■ Health Panel ■ Network Map ■ Service Analyzer ■ Find ■ Home ■ Status ■ Reports ■ Administration	individual Peregrine appliance
Tools	Forecast	map window

In the **Edit** menu, the **Alarm Thresholds** command is always dimmed. The **Alarm Thresholds** command is activated only when there is an associated map window, and the Aggregate Health Panel does not have map windows. Map windows are associated with individual Peregrine appliances.

In the **Tools** menu, two commands are always dimmed:

- **Health Panel**
- **Forecast**

The **Forecast** command, like the **Alarm Thresholds** command in the **Edit** menu, is always dimmed, because there can never be an associated map session.

The buttons in the Tools menu that are active provide the same navigation shortcuts as the Toolbar. Because navigation is associated with the individual Peregrine appliance, these navigation commands provide navigation shortcuts to the Aggregator appliance itself.

Related The pull-down menus of the single-appliance Health Panel are discussed in *Chapter 7, Health Panel Menus*.

7 CHAPTER Health Panel Menus

- To explore commands in pull-down menus, see under the following menus:
  - *File* on page 86
  - *Edit* on page 87
  - *Tools* on page 96
  - *Help* on page 101
- Some Health Panel pull-down menus are similar to those of map windows. You will find similar information in *Chapter 10, Network Map Menus*.
- To learn about the differences between Health Panel pull-down menus and Aggregate Health Panel pull-down menus, see *Pull-down Menus* on page 83.
- To explore parts of the Health Panel windows, see *Chapter 5, Health Panel*.

File

This menu has a single command:

- *Close*

Close

Closes the Health Panel or Aggregate Health Panel.

Related The MIB Browser has a command of the same name. See *Close* on page 278 instead.

Edit

There are two commands in this menu:

- *Alarm Thresholds…* on page 87
- *User Preferences…* on page 88

Alarm Thresholds…

Note: This command is not available to the Aggregate Health Panel.

Note: This command is available only when a Network Map for this Health Panel is open.

Demo, IT Employee: View alarm thresholds for device and alarm types.

IT Manager, Administrator: Set alarm thresholds for all accounts for device and alarm types.

Effects

Warning: When an IT Manager or Administrator changes a threshold, the change affects what everybody sees, even if the IT Manager or Administrator does not use **Save as Prime** (*Save As Prime [Administrator and IT Manager only]* on page 133). Changes take effect *immediately*.

Warning: The **Restore Defaults** button affects all default values.

Options

Table 1: Thresholds

Category	Alarm	Warning
Utilization	YES	YES
Delay	YES	YES
Collisions	YES	YES
Broadcasts	YES	—
Errors	YES	YES
Packet Loss	YES	YES
Changes	YES	—
NEWS	YES	YES
MTTR	YES	YES
MTBF	YES	YES

Limits

Thresholds have little effect on a map window until you select the Health Panel and press one of the fault category buttons.

Procedural alerts

If you enter an alarm threshold that is less critical than the warning threshold, you will be warned.

Related To set *Priority List* on page 72, use the Health Panel.

User Preferences…

Controls how map windows are displayed.

There are three tabs: Map, Health Panel, and Alarm Colors.

Effects

- Updates all map windows immediately.
- Preferences are specific to the account, not the map configuration.

Options Each option is discussed in full below.

Table 2: User Preferences Map options

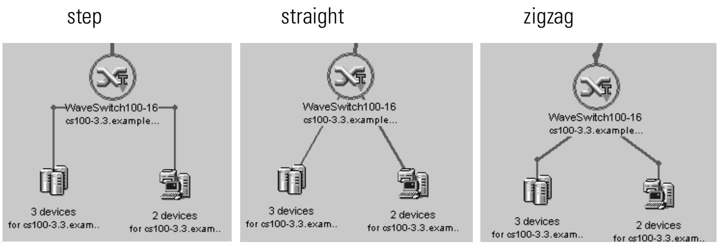
Option	Limits	Default
Map tab		
Line Style	Step | Straight | Zigzag	Straight
Background	Olive | Black | White | Gray	White
Scale	300% | 200% | 150% | 100% | 75% | 50% | 25%	100%
Show pop-up info	On | Off	Off (clear)
Underline locked objects	On | Off	Off (clear)
Confirm packaging commands	On | Off	On (checked)
Shade icons when selected	On | Off	Off (clear)
Show icons when dragging	On | Off	On (checked)
Health Panel tab		
Open Health Panel with Network Map	On | Off	Off (clear)
Use brief Health Panel	On | Off	Off (clear)
Alarm Colors tab		
Alarm Color	Black | Blue | Cyan | Dark Gray | Medium Gray | Green | Light Gray | Purple | Orange | Pink | Red | White | Yellow | Maroon	Red
Warning Color		Yellow
Ok Color		Green
Neutral Color		■ Light Gray (devices) ■ Black (lines)

Line Style

Selects style of connecting lines between objects.

Options Step | Straight | Zigzag

Figure 7-1: Line Style options



Default Straight

Background

Selects background color for map windows.

Effects

- shade of neutral color
- shade of “not seen” color
- shade of “selected” color (when *Shade icons when selected* is checked)

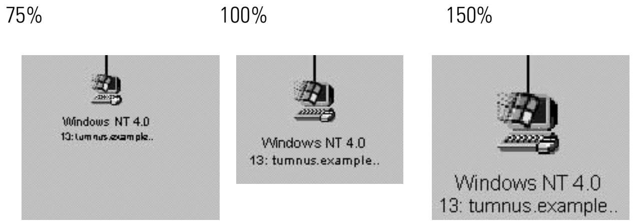
Options Olive | Black | White | Gray

Default White

Scale

Changes the scale at which icons are drawn. The scale is applied to all open map windows and will be applied to all windows that you open subsequently.

Figure 7-2: Map Scale examples



When to use it

- To get an overview of your network, decrease the scale.
- To view a section of your network, increase the scale.
- To increase the amount of blank space in the map window (useful for rearranging groups of objects), decrease the scale.
- To increase the legibility of object titles for projected presentations or for large printed maps, increase the scale. [To print a map, see *Page Setup* on page 134 and *Print…* on page 135.]

Effects

Changing **Scale** affects Print Range—see *Page Setup* on page 134.

Options

300% | 200% | 150% | 100% | 75% | 50% | 25%

Default

100%

Procedural alerts

If you choose a map scale that exceeds your browser memory limitations, the map automatically scales down.

Related

- To change the scale of the current window temporarily (per window), see *Scale* on page 152 in the **View** menu, and *Scale Up* or *Scale Down* on page 153.
- Looking for *Fit Map to Window* or *Fit Window to Map*? See *Scale* on page 152 in the **View** menu.
- To view the object title at smaller scales, position the mouse pointer over the icon until an information box appears. (Assumes that *Show pop-up info* is on.)

Show pop-up info

Toggles whether an information box associated with an object appears when you position the mouse pointer over an icon.

Table 3: Pop-up information box data Health Panel

Information	Real device	Virtual device	Package
Tag	YES	(blank)	YES
Title	YES	YES	YES
Icon	YES	YES	YES
IP address	YES	(blank)	—
MAC address	YES	(blank)	—
Priority	YES	YES	highest device priority within

Default Off (clear)

Underline locked objects

Toggles the underlining of locked objects within all map windows. Objects that are “locked” from a packaging status are shown with a blue line under the icon.

Typically, objects acquire locked status when they are packaged by a user. When an object is locked, Network Discovery does not package or unpackage it.

Default Off (clear)

Related

- To change whether locked objects are underlined temporarily (per window), see *Underline Locked Objects* on page 152.
- To unlock an object, see *Unlock* on page 162.

Confirm packaging commands

Toggles whether commands that affect packaging present a dialog box asking you to confirm your action.

Effects The following commands are affected:

- *Layout* on page 150
- *Pack* on page 150
- *Unpack* on page 151
- *Unpack All* on page 151
- *Unpackage* on page 163

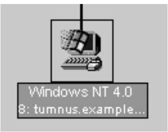
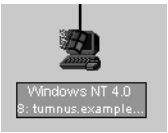
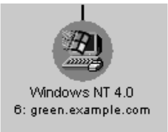
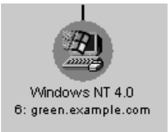
Default On (checked)

Shade icons when selected

There are two methods of indicating:

- selected icons
- “not seen” objects

Table 4: Shaded and non-shaded icons

Icon is...	Not shaded (default)	Shaded
Selected		
Not seen		

Shading icons is more intuitive, but it also requires more memory.

Limits Not available to Windows 95 or Windows 98 management workstations.

Default Off (clear)

Show icons when dragging

Selects how groups of objects are displayed when being moved.

Note: This setting has no effect on groups when they are not in motion.

Note: This setting has no effect on single objects.

When to use it

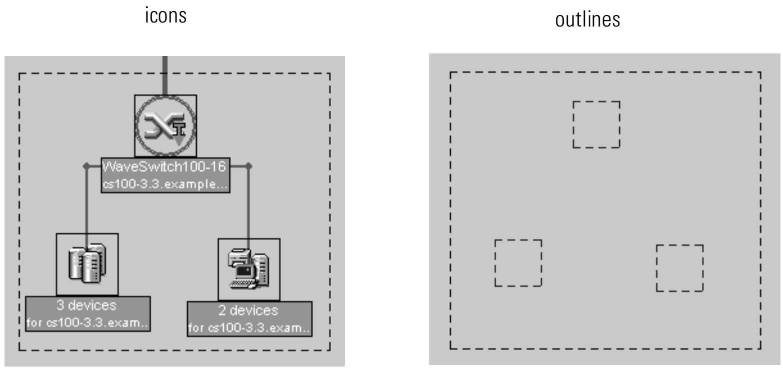
To ensure that a group is dragged smoothly and without flickering images, such as:

- when using a slow computer or video card
- when moving large groups of objects in a densely populated map

Options

On (show icons) | Off (show outlines)

Figure 7-3: Icon group options



Default

On (checked)

Open Health Panel with Network Map

Note: This setting does not affect the Aggregate Health Panel.

Causes the single-appliance Health Panel to be opened automatically whenever you click the **Network Map** button or the **Network Map** command.

Use brief Health Panel

Note: This setting affects both the single-appliance Health Panel and the Aggregate Health Panel.

The Health Panel has two different views, detailed and brief. Detailed is the full Health Panel. This toggles the view you see when you start a map session.

⬆ ⬇ You can switch views at any time by using the arrow button in the bottom right corner of the Health Panel. This setting affects only which view you see initially.

Default

Off (clear)

Related

To switch between views temporarily, see *Switch view* on page 74.

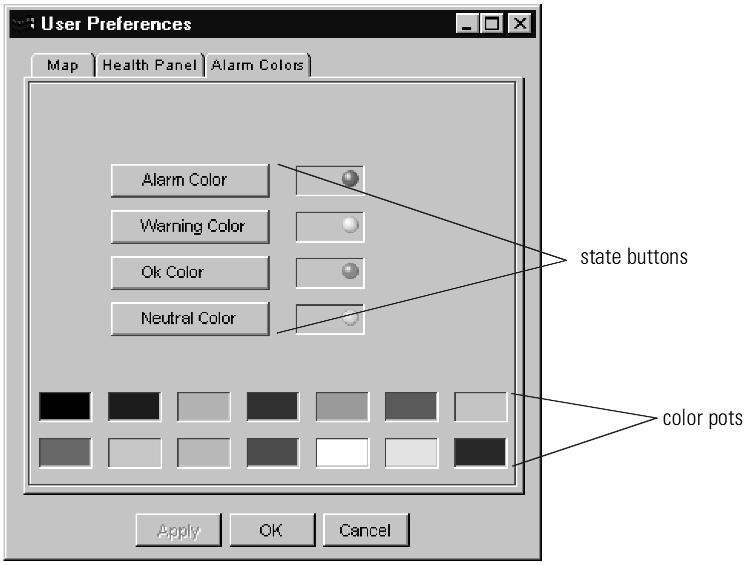
Alarm Colors

Selects colors used to indicate the alarm state of devices, ports, and lines.

Table 5: Alarm colors

Color	Association (default)	Customize
Black	group selection box	—
	Neutral (lines)	YES
Blue	locked object underline	—
Cyan	—	—
Dark Gray	—	—
Medium Gray	“not seen” background	—
Green	OK	YES
Light Gray	Neutral (devices)	YES
Purple	“located” box	—
Orange	—	—
Pink	—	—
Red	Alarm	YES
White	—	—
Yellow	Warning	YES
Maroon	—	—

Figure 7-4: Alarms dialog box



Options

- *state:* Alarm Color | Warning Color | Ok Color | Neutral Color
- *colors:* 14

Limits

Time to apply: up to 40 seconds

Default

Table 6: Default colors

State	Color
Alarm	Red
Warning	Yellow
OK	Green
Neutral (devices)	Light Gray
Neutral (lines)	Light Gray

Tools

This menu provides:

- the same functions as the main Toolbar
- the Health Panel reports
- a shortcut to Health Panel Reports, including a summary of network exceptions (see *Support Reports* on page 276)
- a shortcut to **Status** > **Appliance Health**
- *Forecast* on page 100

Aggregate Health Panel

Opens the Aggregate Health Panel—see *Chapter 6, Aggregate Health Panel*.

Note: *for Aggregator*—Available only when an Aggregator license is present.

Aggregate Events Browser

Opens the Aggregate Events Browser—see *Aggregate Events Browser* on page 262.

Note: *for Aggregator*—Available only when an Aggregator license is present.

List Remote Appliances

Lists the remote appliances—see *Chapter 8, Remote Appliances*.

Note: *for Aggregator*—Available only when an Aggregator license is present.

Health Panel

Open the Health Panel.

Note: Since the Health Panel is already open, this command is never available from within the Health Panel, and is always dimmed.

Note: *for Aggregator*—Not available from the Aggregate Health Panel.

Network Map

- If the Network Map window is closed, this command opens it.
- If the Network Map is open, this command makes it the front-most window.

Note: *for Aggregator*—Not available from the Aggregate Health Panel.

Related To close the Network Map window, see *Close* on page 86.

Service Analyzer

Opens the Service Analyzer—see *Chapter 15, Service Analyzer*.

Note: *for Aggregator*—Not available from the Aggregate Health Panel.

Events Browser

Opens the Events Browser—see *Chapter 16, Events Browser*.

Note: *for Aggregator*—Not available from the Aggregate Health Panel.

Find…

Searches for devices and ports of devices—see *Chapter 17, Find*.

Note: *for Aggregator*—Not available from the Aggregate Health Panel.

Home

Displays the Network Discovery Home page in your web browser—see *Home* on page 40.

Note: *for Aggregator*—Not available from the Aggregate Health Panel.

Status

Opens the Status menu.

Note: *for Aggregator*—Not available from the Aggregate Health Panel.

Reports

Opens the Reports menu—see *Chapter 18, Reports*.

Note: *for Aggregator*—Not available from the Aggregate Health Panel.

Administration

Opens an Administration menu related to your account type.

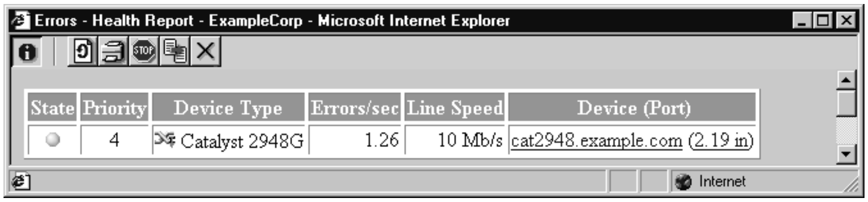
- Admin—see *Chapter 20, Administration for Administrator Accounts*
- Regular—see *Chapter 19, Administration for IT Employee and IT Manager Accounts*
- Demo—the Administration menu is not available

Note: *for Aggregator*—Not available from the Aggregate Health Panel.

Health Panel Reports

All reports provide one row of data for each alarm or warning.

Figure 7-5: Sample Health Panel report


Errors - Health Report - ExampleCorp - Microsoft Internet Explorer
Internet

State	Priority	Device Type	Errors/sec	Line Speed	Device (Port)
○	4	Catalyst 2948G	1.26	10 Mb/s	cat2948.example.com (2.19 in)

The rows are sorted by state, by priority, and by value. The rows of a Line Faults report have two extra columns for data not meaningful in a Device Faults report.

Table 7: Data reported in a Health Panel report

Column	Line	Device	Notes*
State	YES	YES	alarm | warning | ok
Priority	YES	YES	1–6
Device Type	YES	YES	—
Value	YES	YES	see Table 8 on page 98
Line speed	YES	—	in Gb/sec., Mb/sec., kb/sec., or b/sec.
Device	YES	YES	hyperlinked to Device Manager
Port	YES	—	hyperlinked to Port Manager

* The Changes report does not follow this model.

Table 8: Values for a Health Panel report

Category	Value
Line Breaks	Broken since (time/date)
Utilization	Utilization (%)
Delay	Response time (milliseconds)
Collisions	Collisions/sec.
Broadcasts	Frames/sec.
Errors	Frames/sec.
Device Breaks	Broken since (time/date)
Packet Loss	Unicasts formula (%)
NEWS	Days until
MTTR	MTTR (hours)
MTBF	MTBF (days)

When to use it

- If you prefer tabular data over a graphic representation.

- When you want to have a static display of alarms or warnings at a given moment.
- To view all line alarms and warnings, including those that have no line or icon in the Network Map.

Limits No faults affecting devices below the *Priority List* on page 72 are displayed.

Related

- These reports are also available from the Health Panel—see *Reports* on page 97.
- Health Panel reports have a special right-click menu.

Network Exceptions

Provides a shortcut to a summary of network exceptions (*Support Reports* on page 276).

Appliance

Provides a shortcut to **Status** > **Appliance Health**.

Forecast

Note: This command is available only when a Network Map for this Health Panel is open.

Predicts how the network will perform in the future.

Network Discovery computes a probable view of the Network Map based on existing data. Network Discovery assumes that no physical changes will be made to the network. Predictions are made based on the peak busy minute per week, and use linear trends with some data cleaning.

Predictions have three grades of confidence: high, medium, and low. The longer Network Discovery has been running, the more confidence it has in its predictions. Network Discovery is usually most confident about the near future, and less confident about the distant future.

Confidence is based on the number of complete months of network history in the Network Discovery database. (Clearing the database resets the history.)

Table 9: Confidence of Forecast predictions

Confidence	Determining factor
Low	number of months from now > number of months of history accumulated
Medium	3 times number of months from now > number of months of history accumulated
High	3 times number of months from now <= the number of months of history accumulated

Note: The map is always returned to the present when you close the associated map—see *Close Map* on page 138.

Effects

- The progress bar on the Health Panel or the map window’s status bar becomes static and displays the Forecast view instead. Example: “+ 2 months”
- The following commands are disabled:

Table 10: Map menu items disabled by Forecast

Menu	Command
File	New
	Open…
	Open Copy of Prime
	Save
	Save As…
	Save As Prime [admin only]
Object	Reset MTTR and MTBF [admin only]
	Purge [admin only]

Help

Gives two choices, **Network Discovery Help** and **About Network Discovery**. The Network Discovery Help page is the same page that opens from the Toolbar **Help** button. For information on the Network Discovery Help page, see *Help* on page 40, in Chapter 3, *The Toolbar and Other Navigation*.

About Network Discovery

Information about the makers of and modules within Network Discovery. Displayed at the top of the page is the Network Discovery version number.

Ways of opening

- Available as a separate pull-down menu item from the Help button in the Health Panel, in any Network Map window and in the MIB Browser.
- Also available from the Network Discovery Help page.

Related

- For module version numbers, see **Status** > **Current Settings** > **Installed Components.**
- For licenses, **Status** > **Current Settings** > **Installed Licences.**

Procedural Alert

The help button on the About page leads to information about your browser.

8 CHAPTER Remote Appliances

Important: This chapter is only of interest if you have multiple Peregrine appliances in your network, and if the Peregrine appliance you are using is in Aggregator mode.

Remote appliances provide data to an Aggregator appliance. Also, whether providing data or not, all remote appliances can use the Aggregator as a single point of user contact.

The **Home** (or **Home Base**) > **Remote appliances** page is initially empty, since you have not defined any remote appliances for use with the Aggregator.

After you have defined remote appliances, in **Administration** > **Remote appliance administration** > **Add a remote appliance** (see *Add a Remote Appliance* on page 327, the list displays their names and IP addresses. When you click a remote appliance name, you go to the Home page of that Peregrine appliance without having to log in to that appliance.

You assign the name of a remote appliance. We recommend you use the system name of the Peregrine appliance, that is the name used to identify the Aggregator appliance. However, the choice is yours. You can modify the Peregrine appliance name at any time.

Any Peregrine appliance running version IND 4.2 or later or Xanadu 1.0 or later can be a remote appliance. There is no need to apply a special license to an Peregrine appliance to have its data collected by an Aggregator appliance.

Note: Depending on the version, some functions may not be available.

Note: You cannot view a remote appliance from an Aggregator which is running an earlier version of the software; the Aggregator software must be as new as, or newer than the remote appliance.

If a remote appliance is not available, the Aggregator uses the last available imported Health Panel for that remote appliance.

Display

When you view a remote appliance by means of an Aggregator, your user preferences from the Aggregator apply to the display for the remote appliance.

For example, if you have the alarm color defined as red on the Aggregator, but have the alarm color defined as blue on the remote appliance, when you examine the remote appliance, the alarm color is red. If you log in to the remote appliance directly, the alarm color is blue.

If you view a remote appliance through an Aggregator, you see the time set on the remote appliance modified by time zone set on the Aggregator.

For example, you are in Toronto and the time on your Aggregator appliance is set to 12:00. You are viewing a remote appliance in San Diego which has a three-hour time difference. Whoever set the time on the San Diego appliance has it set at 9:05. The time you see on the remote San Diego appliance is 12:05.

Limits

- You must have created an account on the remote appliance that has the same:
  - account name (for example, admin)
  - password (for example, password)
  - account type (for example, Administrator)
- maximum remote appliances: 5
- minimum IND version for data aggregation: 4.2
- minimum Xanadu version for data aggregation: 1.0.4
- maximum Network Discovery version: current version
- If you want to use the Events Browser, the remote appliance must be PND 5.0 or later

Related

- You can also select a remote appliance by using the Toolbar’s *Appliance List* on page 50.
- To create a Aggregator connection to a remote appliance, see *Add a Remote Appliance* on page 327

9 Network Map Window

CHAPTER

- To explore the top and bottom of the window, see *Banner* on page 106 and *Status Bar* on page 107.
- To interpret the icons in a map window, see *Object Appearance* on page 109.
- To explore object position and priority, see *Object Properties* on page 118.
- To understand classification of icons, see *Object Type* on page 119.
- To understand lines, see *Line Appearance* on page 128.
- To explore commands in pull-down menus, see *Chapter 10, Network Map Menus*.

Introduction

Maps consume a large amount of memory, so:

- each Peregrine appliance has a limited number of map sessions
- each account is limited to one map session from the total for the Peregrine appliance

For a detailed explanation, see *Chapter 21, How Network Discovery Works*:

- *Map Session* on page 390
- *Map Configuration* on page 390
- *Map Window* on page 393

There are two types of map window:

- Network Map window
- package window

Table 1: Window differences

Feature	Network Map	Package
Banners	see *Banner* on page 106	
Close on page 138	not available (use *Close Map* on page 138)	available
Promote on page 164	not available (nowhere to promote an object to)	available
Network Map on page 165	not available	available—brings Network Map to front

Banner

The banner, also known as a title bar, may be familiar to you from other applications. The contents of the banner are unique to Network Discovery.

The two kinds of map windows, Network Map and package, have slightly different banners. The label for package windows is more descriptive. The map configuration name (see *Map Configuration* on page 390) appears only in the Network Map banner.

Table 2: Banner elements of map windows

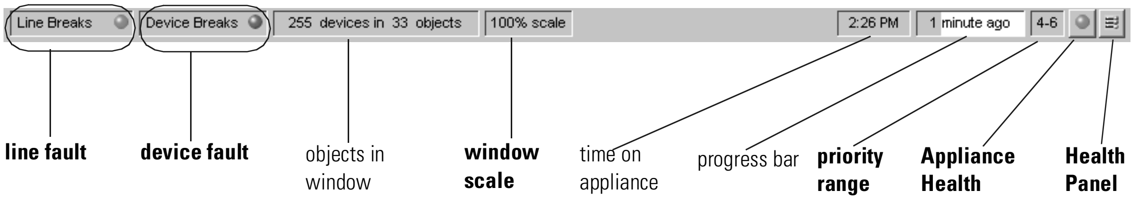
Element	Network Map	Package
window label	Network Map	■ 4 devices for cs1900-01.example.com ■ 3 devices under aslan.example.com ■ MyPackage#1 of 24 devices ■ MyPackage#2 of 9 devices for cs1900-01.example.com ■ MyPackage#3 of 2 devices under aslan.example.com ■ Pkg 4.2.9 of 8 devices
map configuration	(my_map)	—
system name	ExampleCorp	ExampleCorp

Status Bar

The bar at the bottom of the map window displays information about the window and map configuration settings.

Right-click an area to change the setting for the area. (Not all areas support this.)

Figure 9-1: Status bar



Areas that you can right-click are shown in **bold**.

Some areas in the status bar are the same for all map windows within a configuration. These areas are on the right side of the status bar. Other areas change depending on the contents of the window. These areas are on the left side.

Table 3: Elements of the map status bar

Element	Function
■ Line fault category button ■ Device fault category buttons	■ The selected fault category buttons in the Health Panel. To change the selection without returning to the Health Panel, right-click on this area. ■ The selected line fault and device fault are the same for all map windows, but the signal light changes depending on the contents of the window. ■ If all devices within a window are below the minimum priority, the signal light is gray. ■ When disconnected, the signal lights is gray and the buttons can no longer be right-clicked.
Objects in window	The number of devices is the total number available in the window plus in packages available from this window (recursively). The number of objects is the number of icons appearing in the window.
Window scale	The scale at which icons are drawn in this window. To change the scale for this window, right-click on this area.
Time on appliance	The local time for the Peregrine appliance, as entered in **Administration** > **Appliance Management** (*Appliance Management* on page 293). If you view a remote appliance through an Aggregator, you see the time set on the remote appliance modified by time zone set on the Aggregator.

Table 3: Elements of the map status bar (Continued)

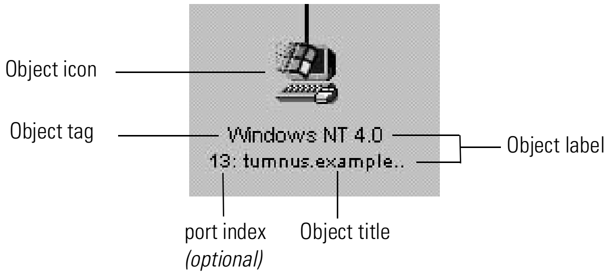
Element	Function
Progress bar	■ The position of the bar indicates both when the data was last refreshed (gray portion), and when it will be refreshed again (white portion). Also, the elapsed time since the data was last refreshed is superimposed on the progress bar. ■ When disconnected, the entire bar is gray and the text reads “Offline”. ■ When *Forecast* on page 168, is being used, the entire bar is gray and the text indicates the prediction period. **Note:** Fast breaks can occur at any time, but do not affect the progress bar.
Priority range	■ The current *Priority List* on page 72. To change the priority, right-click on this area. ■ When disconnected, the area can no longer be right-clicked.
Appliance health	■ The signal light indicates the current health of the Peregrine appliance. To view a detailed report, click this button. ■ When disconnected, the signal light is gray.
Health Panel	To open the Health Panel or to bring the Health Panel forward, click this button.

Object Appearance

For a summary of the object properties that you can change, see *Changing an Object* on page 126.

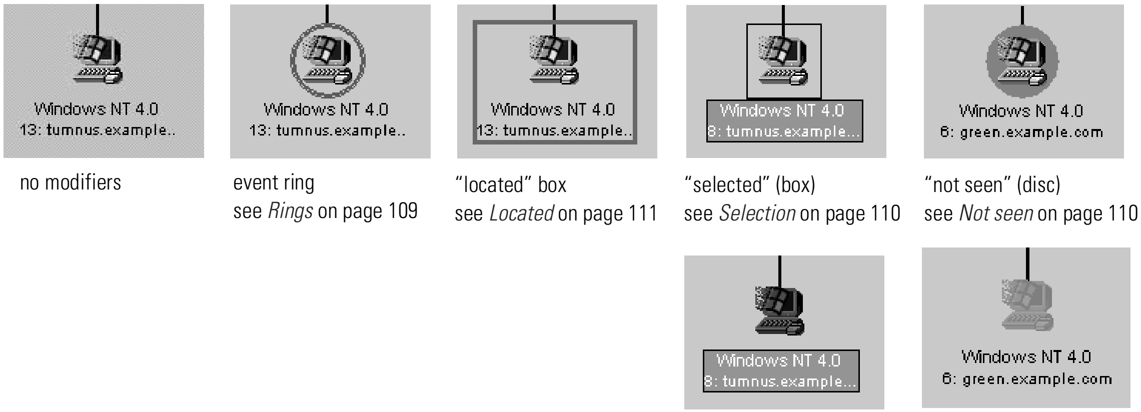
Icon

Figure 9-2: Icon terms



Related See *Label* on page 113.

Figure 9-3: Icon status



no modifiers

event ring
see *Rings* on page 109

"located" box
see *Located* on page 111

"selected" (box)
see *Selection* on page 110

"not seen" (disc)
see *Not seen* on page 110

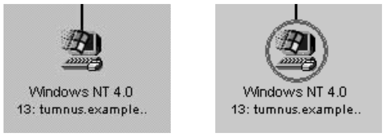
"selected" (shaded)
see *Selection* on page 110

"not seen" (shaded)
see *Not seen* on page 110

Rings

If an object has a ring around it, the Health Panel is monitoring that object for a specific condition.

Figure 9-4: Object monitoring



object not being monitored

object being monitored

The color of a ring reflects the state of an object.

Related

- Changing the color associated with a state is discussed in *User Preferences…* on page 143.

Table 4: Alarm states and colors

State	Default color
alarm	red
warning	yellow
OK	green
neutral	light gray

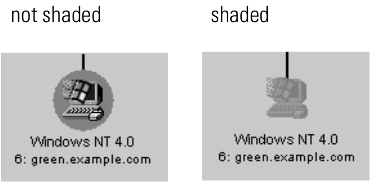
- Changing whether an object has a ring is discussed in *Chapter 5, Health Panel*.

Not seen

An icon with a gray circular background indicates a network device that has not been seen for 24 hours. (Alternately, the device may have a light gray icon—see *Shade icons when selected* on page 146.) Such devices remain on the map until Network Discovery moves them into the trash.

(Scanned-only devices and virtual devices are never considered to be “not seen”.)

Figure 9-5: “Not seen” device



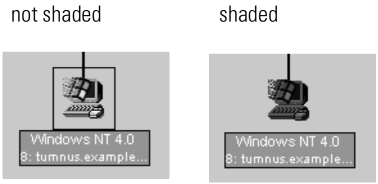
Related

Changing how long “not seen” devices remain on the map is discussed in *Chapter 20, Administration for Administrator Accounts*.

Selection

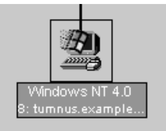
When an object is selected, the icon label is highlighted, and the icon has a box around it. Alternately, the icon may be highlighted in a darker gray—see *Shade icons when selected* on page 146. The exact shade of gray for the highlight color depends on the color of the *Background* on page 144.

Figure 9-6: Selected icons



If more than one object is selected, the group of objects may be surrounded by a black box rendered in broken lines. Whether the black box appears depends on whether the group was created with the mouse or with the Shift key.

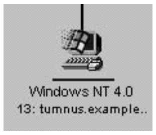
Figure 9-7: Multiple selected icons



Packaged

If an object has been packaged by a user, the “locked” icon is underlined in blue.

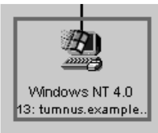
Figure 9-8: “Locked” user-packaged icon



Located

When an object has been located, the object is surrounded by a purple box rendered in thick lines.

Figure 9-9: Located icon



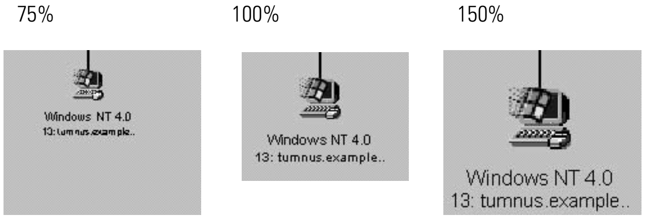
An object can be located as highlighted by:

- using *Find* on page 263
- clicking the Device Manager’s *Locate* on page 198 button
- clicking the Device Manager’s *Properties* on page 204 button
- clicking the Up a Level icon

Scale

Icons can appear in various sizes, depending on the scale percentage selected.

Figure 9-10: Map Scale examples



The scale at which icons are rendered is reflected in the status bar of a map window.

Note: At very small scales, the device label is not shown.

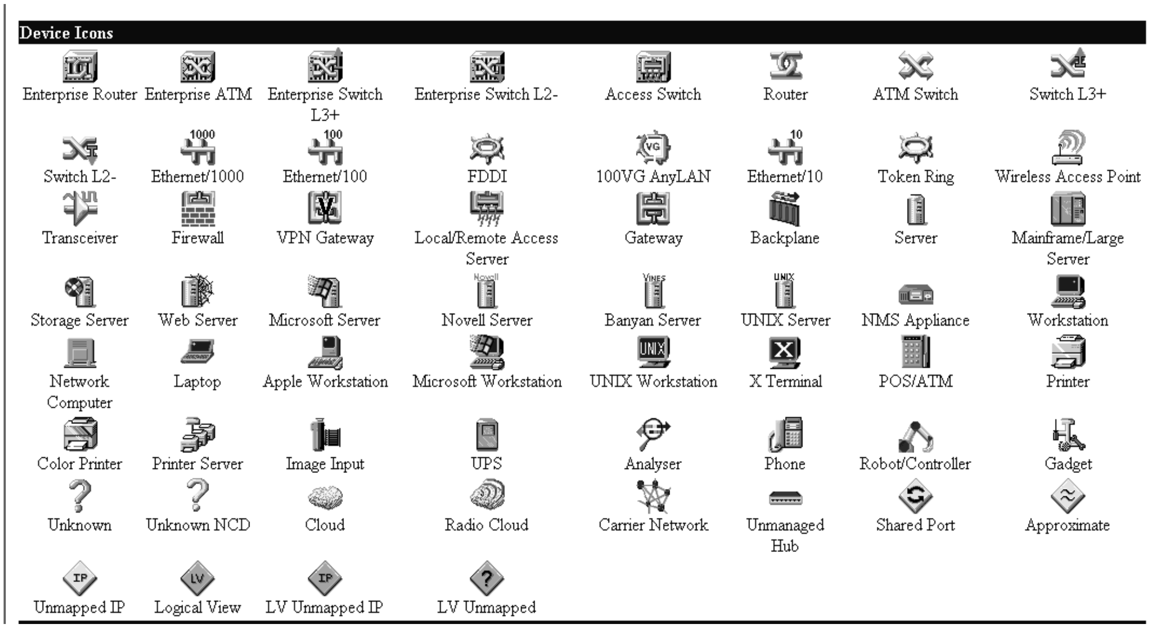
Related

- To change the scale immediately for the active map window, see *Scale* on page 152 or right-click on the scale area of the status bar
- To change the scale for all map windows, see *Scale* on page 144.

Icon type

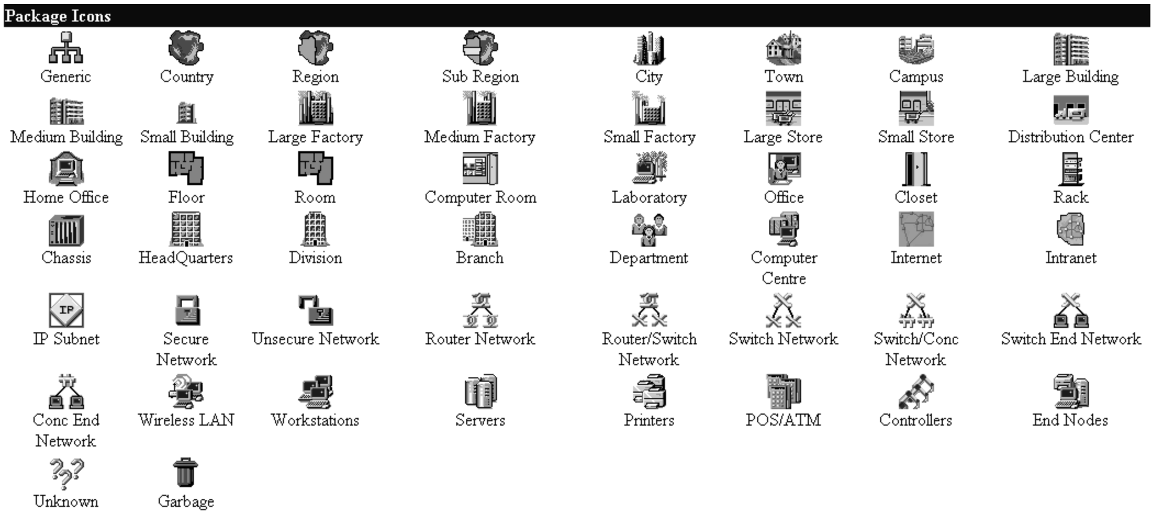
Changing an icon is discussed in *Properties* on page 159.

Figure 9-11: Device icons



Warning: Administrator and IT Manager: Changing a device icon always affects what everybody sees, even if you do not use **Save As Prime**. Changes take effect at the beginning of the next poll cycle.

Figure 9-12: Package icons



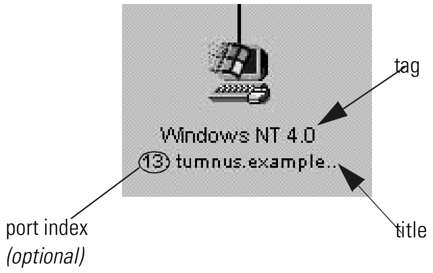
Changing the icon of a package affects only the package’s appearance.

Label

The object label comprises the object tag, object title, and sometimes the object port index.

Note: At very small scales, the device label is not shown.

Figure 9-13: Object label elements



Real device

- device tag further classifies the device (classification is begun by the device icon)
- device title identifies a specific device
- port index identifies the port of the parent device; appears only for icons within an end node package

Virtual device

- no device tag
- device title can identify a subnet or can be arbitrary
- no port index

Package

- package tag shows number of devices contained by package
- package title can identify parent device (end node package) or top object of package (multi-object package); can also be arbitrary (any package)
- no port index

Title

Network Discovery displays only the first 20 characters of a title. If the title is longer than 20 characters, you see the first 18 characters with a suffix of ".." that shows that the title is abbreviated.

Real device

Identifies a real device with a unique identifier. The identifier chosen is based on system preference and data available. For example, an Administrator or IT Manager account user can choose—through **Administration** > **Display Preferences** (*Device Title Preference* on page 369)—to have the identifier be the domain name. If the domain name is available for a specific device, it is displayed. If no device title preferences are available, the IP address or MAC address appears.

Virtual device

The title identifies the subnet ("192.168.96.0/24") or is arbitrary ("Cloud_3"); generated by Network Discovery.

Package

- For a multi-object package, the title is:
  - the device title of the top object within the package
  - arbitrary ("Pkg 9")
- For an node package, the title is:
  - the device title of the parent object with the word, "for", in front of it

Options

The title for a device (real or virtual) is the first available of:

- user-assigned name
- Prime-assigned name
- *virtual devices only:* Network Discovery generated name
- a device title chosen by the Network Discovery Administrator in **Administration** > **Display Preferences** > **Device Title Preference**; (see *Device Title Preference* on page 369). The Network Discovery Administrator can choose one or several of the following and choose their order too:
  - Asset Tag
  - BIOS Asset Tag
  - NetBIOS Name (scan)
  - Last Name
  - First name
  - Device-specific title
  - Domain name
  - NetBIOS name (network)
  - Operating system
  - Family
  - Model

    - Network function
    - System description
    - System name
    - System location
    - System contact
- IPv6 address
- IPv4 address
- MAC address including OUI
- MAC address (all-numeric)

Titles from the Prime configuration are inherited when you open your configuration. The only way to prevent the Prime title from being used is to assign a title yourself by using *Properties* on page 159. You cannot force the use of the default device title instead.

Tag

Real device

A device tag helps to further classify the type of real device. (A virtual device does not have a tag.) Network Discovery assigns the device tag and the device tag cannot be changed.

Table 5: Device tag classes

Tag type	Example
Rule-specific*	Cisco NCD?
Model	Cisco 1601
Family	Cisco 1600
Network Function	Optivity
Operating System	Windows 95
Registered SysObjId Manufacturer	Novell Inc
Registered OUI(MAC) Manufacturer	Cisco

* Limited information is available, or, a managed device is not listed in the Network Discovery Rulebase; see also Table 6.

Table 6: Device tag endings

Ending	Meaning
?	less than 90% probability of identity
NCD?	Network Discovery is relying on the MAC address. The OUI indicates that the device is probably a network connectivity device (NCD), but there is some possibility that it may be an end node.

Package

A package tag identifies the number of devices within the package. Moving devices into and out of packages changes package tags automatically.

Pop-up info

When you position the mouse pointer over an icon, an information box appears. The information box contains the following data.

Table 7: Pop-up information for objects

Information	Real device	Virtual device	Package
Tag	YES	(blank)	YES
Title	YES	YES	YES
Icon	YES	YES	YES
Management	YES	YES (“virtual”)	—
IP address	YES	(blank)	—
MAC address	YES	(blank)	—
Priority	YES	YES	highest device priority within

Table 8: Pop-up information for lines

Information
Line Alarm Type
From
To

When to use it

- When viewing a map window at a reduced scale.
- To determine an object’s priority without opening a Device Manager.

Related To turn this feature on and off, see *Show pop-up info* on page 145.

Object Properties

Position

Position within the window relative to other objects—that is, the x-axis/y-axis position—is a property of the object.

Positioning at the top of the window is a property of windows, but even so, it is controlled with the object's *Properties* on page 159 dialog. See also *Top object* on page 118.

Effects

Adjusting the position of a single object in a window causes all objects within that window to be considered fixed in position.

Related

To "unfix" all objects in a window, see *Layout* on page 150.

Priority

In Network Discovery, devices can have priorities 1–6. Devices with priority 1 are the least important. The higher the number, the higher the priority and greater the importance.

In **Help** > **Device Types**, there is a list of device types and their default priorities.

By default, priorities 5 and 6 are reserved for the user. By default, priority 6 is reserved for those devices that should trigger event notification—see *List Filters* on page 338.

For detailed information, see *Priority* on page 28.

Top object

Whether a given object is the top object in the window or not is a property of the window, not of the object. For detailed information, see *Properties* on page 159.

Limits

For an object to be top object, it must be visible within the window. It cannot be within a package within the window.

Object Type

Network Discovery recognizes two types of objects:

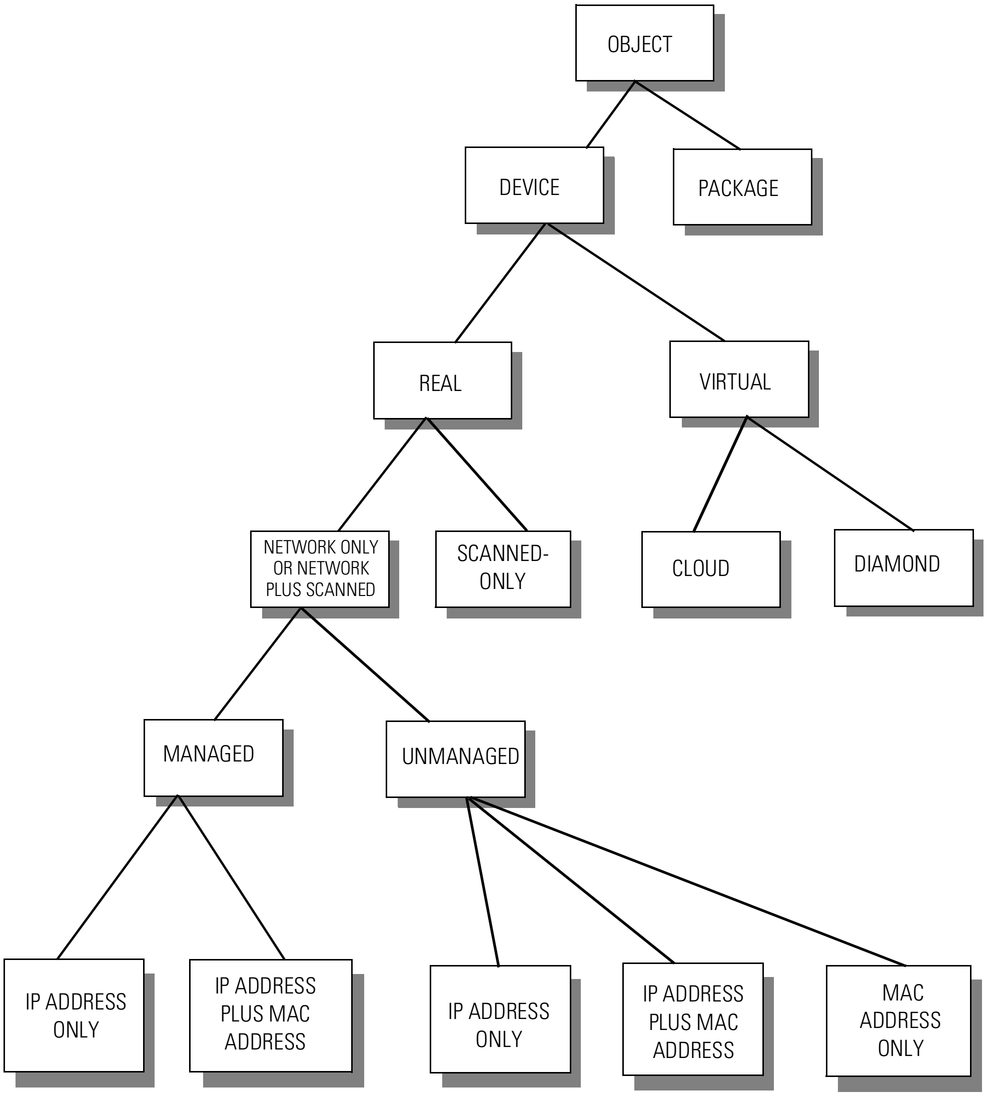
- devices
- packages

Devices are divided into two types:

- real
- virtual

...and so on...

Figure 9-14: Object type hierarchy



Real devices

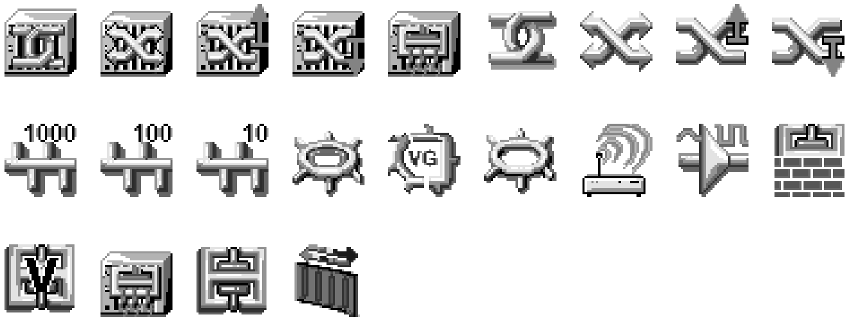
Used when Network Discovery identifies a device and its model.

Network Discovery identifies two principal connectivity classes—network connectivity devices (NCDs) and end nodes.

Network connectivity device (NCD)

A network connectivity device is typically a router or switch.

Figure 9-15: Network connectivity device icons



When Network Discovery can partially identify a device and believes it to be a network connectivity device (such as a router or switch), it uses the yellow Unknown NCD icon.

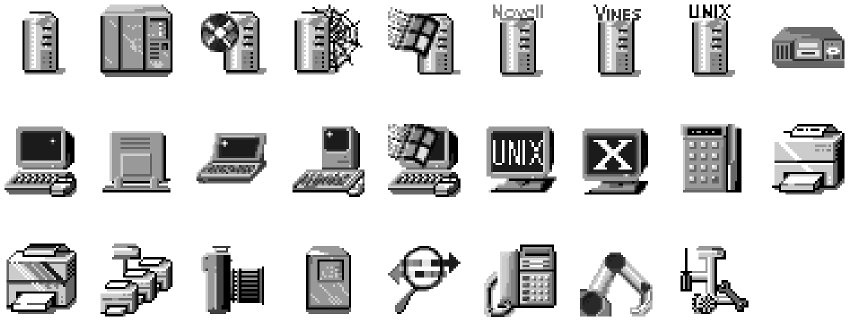
If Network Discovery is uncertain whether a device is a network connectivity device, it adds “NCD?” to the end of the tag.

Note: A phone icon is usually treated as an end node, but can also be treated as a connectivity device.

End node

An end node is typically a server, workstation, or some input device (like a an image scanner) or output device (like a printer). An end node has a single connection.

Figure 9-16: End node icons



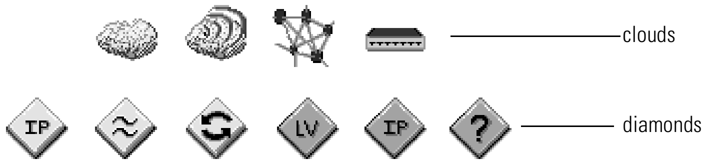
When Network Discovery cannot identify a device to any degree whatsoever, it uses the gray Unknown icon.

Virtual devices

When Network Discovery is unable to determine the exact physical, port-level connectivity between devices, it represents the connection (or connections) using a virtual device. Virtual devices come in two types:

- cloud
- diamond

Figure 9-17: Virtual device icons



Cloud virtual devices

Clouds are used to represent a real device—or several real devices—that Network Discovery cannot yet identify.

Table 9: Cloud virtual devices

	Virtual device type:	Cloud
	Map title:	default cloud
	Objects represented:	one or more unmanaged devices
	Connected to:	two or more devices
	Virtual device type:	Radio Cloud
	Map title:	radio
	Objects represented:	fixed and mobile wireless devices
	For which Network Discovery:	has determined that an end node is employing one or more Wireless Access Points
	Virtual device type:	Carrier Network
	Map title:	carrier
	Objects represented:	a third-party network composed entirely of unmanaged devices
	Relationship:	with a physical connection
	For which Network Discovery:	has determined the interface type to be SMDS, SONET, IEEE 802.6, CATV, and so on

Table 9: Cloud virtual devices (Continued)

▬	*Virtual device type:*	Unmanaged Hub
	Map title:	unmanaged hub
	Objects represented:	a single hub device
	Relationship:	that connects two or more devices
	For which Network Discovery:	cannot read the MIB

Diamond virtual devices

Diamonds are used to represent connections that Network Discovery has identified but has not yet determined precisely. Since a diamond icon represents a connection and not a physical object, a diamond is a more theoretical object than a cloud.

Table 10: Diamond virtual devices

IP	*Virtual device type:*	Unmapped IP
	Map title:	one of: ■ multiple lsns <#> ■ *<subnet>* / *<netmask_CIDR>* (for example,192.168.1.0/18) ■ approximate lsn <#>
	Objects represented:	a collection of devices
	Relationship:	that belong on the same logical subnet
	For which Network Discovery:	has not yet determined the physical connection
≈	*Virtual device type:*	Approximate
	Map title:	unknown ports
	Objects represented:	a port on a switch or hub
	Connected to:	both: ■ a switch or hub ■ two or more end nodes or virtual devices
	For which Network Discovery:	has not yet determined the exact port index on the switch or hub

Note: You cannot deduce the existence of all approximate connections by looking for Approximate diamonds on the map. No Approximate diamond is created for approximate connections between a switch or hub and one other single object (whether end node or virtual device).

Table 10: Diamond virtual devices (Continued)

⟳	*Virtual device type:*	Shared Port
	Map title:	shared port
	Objects represented:	multiple devices
	Relationship:	attached to a single port
	For which Network Discovery:	is seeing one device at a time off the port, rather than multiple devices concurrently
LV	*Virtual device type:*	Logical View
	Map title:	logical view
	Objects represented:	a special object
	Connected to:	■ Always connected to: ■the Peregrine appliance icon ■all logical subnets for which no connection is known ■ May be connected to devices to which the connection has been broken, where there are no other places to connect it
	Note: The Logical View object always has at least two icons attached: one LV Unmapped IP icon and the Peregrine appliance icon.	
IP	*Virtual device type:*	LV Unmapped IP
	Map title:	■ *<subnet>* / *<netmask_CIDR>* (for example, 192.168.1.0/18) ■ unknown lsns
	Objects represented:	a collection of devices
	Relationship:	that belong on the same logical subnet
	For which Network Discovery:	has not yet determined the physical connection or the associated router
?	*Virtual device type:*	LV Unmapped
	Map title:	unknown lsns
	Objects represented:	a collection of devices
	Relationship:	for which the logical subnet is unknown

Packages

There are two types of packages:

- multi-object packages
- end node packages

Multi-object packages can be created by Network Discovery or by you. When Network Discovery creates packages, it always determines the initial contents (which you can change afterward). Also, the contents of these packages are not locked. When you create packages, you have direct control over the contents, but the contents of the packages are considered locked.

End node packages are always created by Network Discovery. The contents of end node packages are not locked. For details, see *Default end node packages* on page 124. For details on customizing, see **Administration** > **Display preferences** > **Automatic packaging** (*Automatic Packaging* on page 372).

When package icons have colored rings, the ring reflects the most severe state of all objects contained in the package. For example, if there are alarm, warning, and OK rings within the package, the package has an alarm ring.

A package tag is “X devices”, where X represents the total number of devices. When devices are moved out of or into a package, Network Discovery updates the number to reflect the contents.

Limits

Maximum packages: 2500

Related

- For information on why objects are locked and what it means, see *Underline locked objects* on page 145.
- To lock or unlock an object, see *Lock* on page 161 or *Unlock* on page 162.

Default package

The default package created by the *Pack* on page 150, *Create Package* on page 152, and *Package* on page 164 commands when the contents are various classes of object.

Default end node packages

The default package created (as a side effect by the **Unpack All** command) when the contents are end nodes of various classes. An end node has a single connection, and is not a network connectivity device (such as a switch or router).

Icons in end node packages are displayed with reference to the upstream device. The icon attached to port 1 will be first in the package window, and so on.

If the end nodes are of the same class—for example, all workstations—then a special end node package may be created.

Table 11: Classes of end node package

Icon	Class
	Workstations
	Printers
	Servers
	POS/ATM
	Controllers
	Unknown
	End Node

The title of an end node package always begins with “for”.

Related To change how and when end node packages are created, see *Automatic Packaging* on page 372.

New Package

The New Package is intended for you to place objects in. It uses the default package icon.

You cannot open the New Package, because it is empty. You can have one New Package in a map window at a time. When you put something into a New Package, its name changes. The new name begins with “Pkg”.

The only **Object** menu commands available to the New Package are **Unpackage** and **Promote**. These are the only commands available to any empty package.

Up a Level

The “Up a Level” icon is neither a device icon nor a package icon. You can use it to change the active map window. You can also use it to promote an object by dragging the object on top of it.

Changing an Object

The effects of customizing an object's appearance depends on your account type.

Note: Changing a device icon affects much more than its appearance.

IT Employee and Demo accounts

When you make changes to a map configuration, the changes only ever apply to that one configuration. Your other configurations, and the configurations of other accounts cannot be affected.

Table 12: Changing objects—IT Employee and Demo accounts

To change	Do this
icon—devices	contact Network Discovery Administrator
icon—packages	see *Properties* on page 159
tag	—*
derived title (devices)	contact Network Discovery Administrator
title	see *Properties* on page 159
priority (devices)†	see *Properties* on page 159
position	see *Position* on page 118
to top object	see *Top object* on page 118

* The tag is set by the Network Discovery Rulebase and cannot be changed. If it is incorrect, contact Customer Support.

† Changing priority does not affect whether you receive a page or an e-mail about a device.

Administrator and IT Manager accounts

When you make changes to a map configuration, the changes have the potential to affect all accounts and all configurations.

Table 13: Changing objects—Administrator and IT Manager accounts

To change	Do this	Affects other accounts and maps	Also affects
icon—devices	see *Properties* on page 159	YES	■ thresholds (all accounts) ■ whether event filters are applied (all accounts) ■ reports
icon—packages	see *Properties* on page 159	n/a	n/a
tag	—*	—	—
derived title (devices)	see *Device Title Preference* on page 369	YES	—
title	see *Properties* on page 159	only if saved to Prime	—
priority (devices)	see *Properties* on page 159	only if saved to Prime	whether event filters are applied (all accounts)
position	see *Position* on page 118	only if saved to Prime	—
to top object	see *Top object* on page 118	only if saved to Prime	—

* The tag is set by the Network Discovery Rulebase and cannot be changed. If it is incorrect, contact Customer Support.

Line Appearance

This section deals solely with the way a line is rendered within a map window.

To change the priority of a line, change the priority of one of the devices at its endpoints. See *Properties* on page 159 or *Properties* on page 204.

Administrator or IT Manager: To change the Network Discovery perception of a line type, see *Interface Type [Administrator or IT Manager only]* on page 222.

Color

When the Health Panel has no Line Fault buttons selected, lines are the neutral color. (By default, the neutral color for lines is black.)

When there is a Line Faults button selected, the color of a line reflects the state of the line with respect to *Priority List* on page 72.

Related Changing the color associated with a state is discussed in *User Preferences…* on page 143.

Table 14: Line states and colors

State	Default color
alarm	red
warning	yellow
OK	green
neutral	light gray

Thickness

The thickness of a line reflects its capacity. There are two thicknesses:

- thin for less than 100 Mbit
- thick for greater than 100 Mbit

Style (hierarchy)

There are three line connection styles:

- Step
- Straight
- Zigzag

Related Changing the connection style is discussed in *User Preferences…* on page 143.

10 CHAPTER Network Map Menus

- To explore commands in pull-down menus, see under the following menus:
  - *File* on page 130
  - *Edit* on page 142
  - *View* on page 150
  - *Object* on page 155
  - *Tools* on page 165
  - *About Network Discovery* on page 169
- To explore right-click menus, see *Right-click Menus* on page 170.
- To explore parts of the Network Map windows, see *Chapter 9, Network Map Window*.

Introduction

Maps consume such a large amount of memory, so:

- each Peregrine appliance has a limited number of map sessions
- each account is limited to one map session from the total for the Peregrine appliance

File

- *New* on page 131
- *Open…* on page 131
- *Open Copy of Prime* on page 131
- *Save* on page 132
- *Save As…* on page 132
- *Save As Prime [Administrator and IT Manager only]* on page 133
- *Page Setup* on page 134
- *Print…* on page 135
- *Session Info* on page 136
- *Disconnect* on page 136
- *Reconnect* on page 137
- *Close* on page 138
- *Close Map* on page 138

Note: For information on map configurations, see *Map Configurations* on page 140.

New

Creates a new map configuration based on the default Network Discovery configuration. Has the name "Untitled" until you save it.

Effects Closes all open map windows. The Network Map window is completely repopulated and redrawn.

Limits Not available when using the **Forecast** command to view the Network Map.

Related

- To start with a previously saved map configuration file, see *Open…* on page 131.
- To refresh the window, see *Layout* on page 150.

Open…

Opens a map configuration file from your account area.

There are two shortcuts available:

- Copy of Prime appears at the top of the list (same as *Open Copy of Prime* on page 131)
- a check box for a untitled map with default packaging appears below the list (same as *New* on page 131)

Effects Once you select a map configuration to open, Network Discovery closes all open map windows. The Network Map window is completely repopulated and redrawn.

Limits Not available when using the **Forecast** command to view the Network Map.

Related

- To start a new configuration, see *New* on page 131.
- To start a new copy of the Prime configuration, see *Open Copy of Prime* on page 131.

Open Copy of Prime

Opens a copy of the Prime configuration:

- packaging
- layout
- top objects
- icons (packages)
- titles (all objects)
- priorities (devices)

Limits Not available when using the **Forecast** command to view the Network Map.

Related

- Alternative: From the **File** menu, click **Open…**, then click the check box for a untitled map with default packaging.
- Administrator and IT Manager: To make changes to the "Prime" configuration, see *Save As Prime [Administrator and IT Manager only]* on page 133.

Save

Saves your map configuration using the current name.

When to use it

- To store a condition to which you can return
- Before exiting the Health Panel
- Before making major changes to the map (such as using the **Unpack** or **Pack** commands)
- Before using *Disconnect* on page 136
- After using *Properties* on page 159

Effects

Deletes the autosave configuration.

Limits

Not available when using the **Forecast** command to view the Network Map.

Procedural alerts

- Always **Save** before you *Close Map* on page 138.
- Always **Save** before you *Disconnect* on page 136.

Related

To save a configuration under a different name, see *Save As…* on page 132.

Save As…

Saves your map configuration using a different name. Can be used to create a new configuration file or to overwrite an existing configuration file.

You can select an existing name from the list, or type a new name in the box.

Limits

Not available when using the **Forecast** command to view the Network Map.

Table 1: Map configuration name characteristics

Characteristic	Limits
Length	1–30 characters*
Valid characters	A–Z, a–z, 0–9, _ (*underscore*), - (*hyphen*)
Case sensitive	yes

* The date- and time-stamp are not part of the name, and do not count against the 30-character limit.

Table 2: Map configuration name examples

Example	Explanation
Acceptable names	
simple	—
FirstTry	—
my_map	—
2001-05-09_global	—

Table 2: Map configuration name examples (Continued)

Example	Explanation
Unacceptable names	
I_like_the_way_this_config_looks	too long
example.net	uses illegal period
My Config	uses illegal space

Effects Deletes the autosave configuration.

Procedural alerts Configuration names are case sensitive. “Simple”, “simple”, and “SIMPLE” are three different configurations.

Related To save a configuration under its current name, see *Save* on page 132.

Save As Prime [*Administrator and IT Manager only*]

Saves current configuration to the Prime configuration:

- packaging
- layout
- top objects
- icons (packages)
- titles (all objects)
- priorities (devices)

Important: There can be more than one Administrator and or IT Manager account. Two or more Administrator and or IT Manager accounts can access Network Discovery simultaneously. In this situation, there is a risk of one account overwriting the work of another account.

Effects

- The current configuration name:
  - is unchanged, if the configuration already had a name
  - is changed to Prime, if the configuration had been untitled
- May alter the effectiveness of event filters (if any device priorities have changed and if any event filters have priority as a selection criterion).
- May affect the Events Browser.
- Affects device titles.

Limits Not available when using the **Forecast** command to view the Network Map.

Page Setup

Adjusts appearance of printed maps. Includes a page preview.

When to use it

- To adjust paper size or positioning.
- To customize the header and footer of the printed page.
- To select the tiles that are printed.
- To adjust the layout of the map window (relative to printed page breaks).
- To adjust the scale of the map window for printing.

Effect

Blue lines appear in the active map window as long as you have the Page Setup window active.

Options

Three options (paper size, orientation, and range) should be familiar. The page header and footer values may be less familiar, but are used by some web browsers.

Table 3: Page Setup options

Values	Notes	Example
	Orientation	
Portrait	—	—
Landscape	—	—
	Paper Size	
Executive (7¼"×10½")	—	—
Letter (8½"×11")	—	—
Legal (8½"×14")	—	—
Large (11"×17")	—	—
A3 (297mm×420mm)	—	—
A4 (210mm×297mm)	—	—
A5 (148mm×210mm)	—	—
B4 (210mm×297mm)	—	—
B5 (210mm×297mm)	—	—
Dolev800 (30"× 40")	—	—
	Page Header and Footer	
Window Name	name of map window; at header left	Network Map
Network Name	system name (see *Appliance System Variables* on page 294); at header center	ExampleCorp
User.Config	account name and configuration name; at header right	dupont.my_map
Tile Number	current and total tile numbers; at footer left	Tile (2,1) of (1,1)...(4,3)
Page Number	current and total page numbers; at footer center	Page 1 of 12
Date Printed*	date and time when map was printed; at footer right	Tue Jun 29 16:08:59 EDT 1999

Table 3: Page Setup options (Continued)

Values	Notes	Example
Tile Marks	registration marks to help you to attach pages; in header and footer	
	Print Range	
All	print the entire map	
Tiles	print a portion of the map	2,1 to 4,1

* Not affected by setting *Account Properties* on page 282.

Tiles are expressed in columns and rows. The tile 3,2 is the third tile across and the second tile down:

1,1	2,1	3,1	4,1
1,2	2,2	**3,2**	4,2
1,3	2,3	3,3	4,3

Note: If you use *Scale* on page 152 to change window scale between printings, tiles defined in the print range cover completely different areas.

Tip: If you want to tape or glue all the pages together after printing to create an overview, turn on the Tile Marks. These marks act as a guide.

Note: These options do not override the printer properties for the printer attached to your management workstation.

Procedural alerts

- Check that the printer settings match the printer properties.
- Turn off duplex in your printer properties. You will usually want to print maps single-sided.

Related

To print without setting up the page, see *Print…* on page 135.

Print…

Prints the map window.

The window is printed using the current page setup and the printer properties for the printer attached to your management workstation.

Procedural alerts

Note: *for Netscape*—The first time you print, you will be asked to grant permission.

Related

To adjust the appearance of the page before printing, see *Page Setup* on page 134.

Session Info

Provides information about your map session, including:

- Network name—see system name in *Appliance System Variables* on page 294 in *Chapter 20, Administration for Administrator Accounts*
- Domain name and IP address of the Peregrine appliance, plus the port of the Peregrine appliance being used for the map session
- Version number of Network Discovery running on this Peregrine appliance
- Account name, which is the name you used when you logged in—see "Logging In to the Peregrine Appliance" in the *User Guide*
- Date and time of current connection
- Number of map session, including reconnects, whether requested by the account or not (see *Reconnect* on page 137)
- Configuration name; see *Save As…* on page 132
- IP address of your management workstation
- Active web browser on your management workstation
- Version number of map client applet
- Date and time of original connection by map client applet

Disconnect

Suspends your map session without closing map windows or saving your configuration file. Frees up a map session for use by another account.

When to use it

If you want to:

- suspend and print the current state of the Network Map
- avoid having to quit and restart, particularly when you must leave your map session for only a short time
- prevent reconnection attempts to an Peregrine appliance you know is unavailable

If you must:

- free up a map session at the request of another account

Effects

- Once you disconnect, map windows become static. Faults and changes to the network and its objects are no longer displayed. You can change the display of open map windows but not the contents (such as packaging).

Table 4: Effects of Disconnect command on Network Map

Class of tasks	Effect
Tasks that work the same	printing a map window
	scaling a map window
	scrolling a map window
	opening a Device Manager window
Tasks that work differently	moving an object in open map windows (object may not stay in position)
Tasks you cannot perform	opening a map window
	opening a package
	packaging / unpackaging objects
	saving / opening a configuration file
	opening a Line Manager window

- The map status bar changes as follows:
  - The Line fault and Device fault category button signal lights are gray and the buttons can no longer be right-clicked.
  - The progress bar is gray and the text reads “Offline.
  - The priority area can no longer be right-clicked.
  - The Appliance button’s signal light is gray.

Procedural alerts

- Always **Save** your map configuration before you **Disconnect**.
- This command is not available when the map session is already disconnected.

Related

- To return to a suspended map session, see *Reconnect* on page 137.
- To end a map session, see *Close Map* on page 138.

Reconnect

Re-establishes and resumes your map session after a disconnection.

Important: If you are already connected, **Reconnect** first disconnects, then reconnects.

When to use it

- If you have suspended your session with the **Disconnect** command and now want to resume it.

- If an Administrator account disconnected you from your session. (See **Status** > **Network Map Sessions**)
- If you have been disconnected from the Peregrine appliance in some other way. For example, if the Peregrine appliance was turned off for maintenance but has now been turned back on.

Effects

Each time you click the **Reconnect** command, Network Discovery makes several attempts to reconnect, not just one. A complete reconnection cycle can be over in a few seconds, or can continue for over an hour.

A dialog box appears and informs you of the progress of the attempt to reconnect. If the dialog box disappears before you can read it, that means the connection is made.

Once a connection is made, all open map windows are refreshed with the most recent data. Manager windows are not refreshed. No map windows are closed.

If Network Discovery fails to make a connection, the progress messages in the dialog box should help to diagnose the problem.

Procedural alerts

Demo: Always **Save** your map configuration. When you **Reconnect**, you will be given a Copy of Prime. To recover your map configuration after a reconnection, you need to **Open…** it.

Related

- To suspend a map session, see *Disconnect* on page 136.
- To end a map session, see *Close Map* on page 138.
- To view the number of successful reconnections, see *Session Info* on page 136.

Close

Closes the current map window.

Related

- To re-open a package window, double-click the icon for the package.
- To close more than one map window, see *Close Map* on page 138 or *New* on page 131 or *Open…* on page 131.
- The MIB Browser has a command of the same name. See *Close* on page 278 instead.

Close Map

Closes all map windows and ends the map session.

Note: Ending a map session is not the same as logging out of Network Discovery.

Effects

- Manager windows are left open.
- The name of the current map configuration is stored (so that the configuration can be loaded automatically the next time you open a Network Map).
- The map is returned to the present and the Forecast dialog box is closed.

Procedural alerts

- Always *Save* on page 132, before you **Close Map**.

- If your map configuration has not been saved, you are asked if you want to save it now.
- If you are not asked to save your configuration, you are asked to confirm the action of exiting.

Related

- To suspend a map session, see *Disconnect* on page 136.
- To begin a new map session, click the main Toolbar's **Network Map** button, or from the Health Panel, click *Network Map* on page 96.
- To log out of Network Discovery altogether, click the main Toolbar's **Exit** button.

Table 5: Windows closed by various commands

	File pull-down menu		Toolbar
Windows	**Close Map**	**Close**	**Exit**
map windows	YES	YES	YES
Health Panel	—	YES	YES
Health Panel reports	—	YES	YES
dialog boxes	some	YES*	YES
Manager windows	—	YES	YES
Toolbar	—	—	YES

* Except those windows belonging to external applications; for example, Telnet.

Map Configurations

Network Discovery automatically opens a map configuration file at the start of each map session. The first time a new account starts a map session, this is always a copy of the Prime configuration. All other times, the map configuration file that Network Discovery opens depends the type of account you are using.

Table 6: Default configuration files and accounts

Account type	Subsequent default file
Demo	Copy of Prime
IT Employee	last opened or designated
IT Manager	last opened or designated
Administrator	last opened or designated

When you end a map session, Network Discovery takes note of what map configuration file is in use. The next time you start a map session, Network Discovery opens that file. There are two exceptions:

- You can designate a different configuration file to be opened next time. See *Manage Map Configurations* on page 290.
- Demo accounts always start a map session with a configuration called “Copy of Prime”. This is so that each user of a Demo account can start fresh, unaffected by previous users.

  Demo accounts can open a saved configuration if they want to pick up where they left off.

Related See also *Map Configuration* on page 390.

Prime configuration

The Prime configuration is a special configuration not associated with a particular account. This configuration is customized and maintained by Administrator or IT Manager-level accounts.

Any Administrator or IT Manager account can overwrite the Prime configuration. To do so, see *Save As Prime [Administrator and IT Manager only]* on page 133.

The Prime configuration includes:

- packaging
- layout
- top objects
- icons (packages only)
- titles (all objects)
- priorities (devices)

Important: The Prime configuration in general—and its priorities in particular—control *Notification and Events Configuration* on page 328, the *Events Browser* on page 257, and most reports.

Note: One Prime configuration setting cascades down to the configurations of other accounts: default titles (all devices)

This setting is used unless the owner of a configuration has changed the title of a device.

Table 7: Cascade of device titles from Prime configuration

Prime-assigned title	Account-assigned title	What the account owner sees
website	CorpWebSite	CorpWebSite
website	—	website

Device priority from the Prime configuration does not cascade to any other configurations. However, device priority does affect Notification and Events Configuration.

The default Prime configuration has end node packaging—all core devices are in the Network Map window. Layout, device priorities, and titles are all set to the default.

If you end your session with “Copy of Prime”, you will get a fresh copy of Prime the next time you start a map session.

Autosave

Configuration files are saved automatically every 2 minutes (or more frequently). This makes it possible for you to recover your configuration in the event of an abnormal occurrence, such as a disconnection from the Peregrine appliance or a power outage.

If a session ends abnormally, the recovery file opens the next time you start a map session, and you will be notified of the recovery with a dialog box: “Restored configuration from autosave”.

Even when Network Discovery loads the recovery file, you can still discard the recovery. Just re-open the configuration file that you last saved.

Note: Autosave never overwrites any configuration file that you have created. The autosave file is deleted any time you answer “No” to the question “Do you want to save the changes?”. The autosave file is also deleted every time you save a configuration.

Important: Always *Save* your map configuration before you *Close Map*. Do not rely on Network Discovery being able to recover the autosave file.

Edit

There are two commands in this menu:

- *Alarm Thresholds…* on page 142
- *User Preferences…* on page 143

Alarm Thresholds…

IT Employee, Demo: View alarm thresholds for device and alarm types.

Administrator or IT Manager: Sets alarm thresholds for all accounts for device and alarm types.

Effects

Warning: Changing a threshold always affects the configurations of all accounts, even if **Save As Prime** [Administrator or IT Manager only] is not used. Changes take effect *immediately*.

Warning: The **Restore Defaults** button affects all default values.

Options

Table 8: Thresholds

Category	Alarm	Warning
Utilization	YES	YES
Delay	YES	YES
Collisions	YES	YES
Broadcasts	YES	—
Errors	YES	YES
Packet Loss	YES	YES
Changes	YES	—
NEWS	YES	YES
MTTR	YES	YES
MTBF	YES	YES

Limits

Thresholds have little effect on a map window until you select the Health Panel and press one of the fault category buttons.

Procedural alerts

If you enter an alarm threshold that is less critical than the warning threshold, you will be warned.

Related

To set *Priority List* on page 72, use the Health Panel.

User Preferences…

Controls how map windows are displayed.

There are three tabs: Map, Health Panel, and Alarm Colors.

Effects

- Updates all map windows immediately.
- Preferences are specific to the account, not the map configuration.

Options

Each option is discussed in full below.

Table 9: User Preferences Map options

Option	Limits	Default
Map tab		
Line Style	Step | Straight | Zigzag	Straight
Background	Olive | Black | White | Gray	White
Scale	300% | 200% | 150% | 100% | 75% | 50% | 25%	100%
Show pop-up info	On | Off	Off (clear)
Underline locked objects	On | Off	Off (clear)
Confirm packaging commands	On | Off	On (checked)
Shade icons when selected	On | Off	Off (clear)
Show icons when dragging	On | Off	On (checked)
Health Panel tab		
Open Health Panel with Network Map	On | Off	Off (clear)
Use brief Health Panel	On | Off	Off (clear)
Alarm Colors tab		
Alarm Color	Black | Blue | Cyan | Dark Gray | Medium Gray | Green | Light Gray | Purple | Orange | Pink | Red | White | Yellow | Maroon	Red
Warning Color		Yellow
Ok Color		Green
Neutral Color		■ Light Gray (devices) ■ Black (lines)

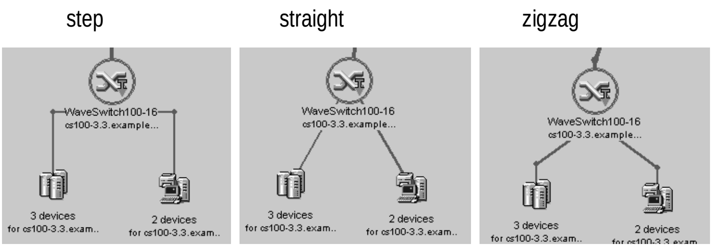
Line Style

Selects style of connecting lines between objects.

Options

Step | Straight | Zigzag

Figure 10-1: Line Style options



Default Straight

Background

Selects background color for map windows.

Effects

- shade of neutral color
- shade of “not seen” color
- shade of “selected” color (when *Shade icons when selected* is checked)

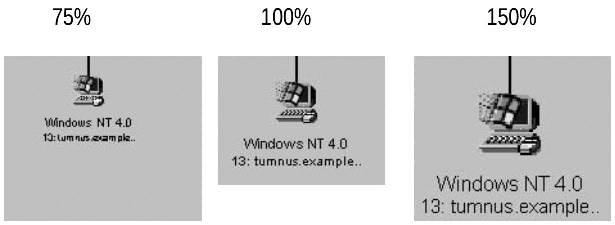
Options Olive | Black | White | Gray

Default White

Scale

Changes the scale at which icons are drawn. The scale is applied to all open map windows and will be applied to all windows that you open subsequently.

Figure 10-2: Map Scale examples



When to use it

- To get an overview of your network, decrease the scale.
- To view a section of your network, increase the scale.
- To increase the amount of blank space in the map window (useful for rearranging groups of objects), decrease the scale.
- To increase the legibility of object titles for projected presentations or for large printed maps, increase the scale. [To print a map, see *Page Setup* on page 134 and *Print…* on page 135.]

Effects Changing **Scale** affects Print Range—see *Page Setup* on page 134

Options 300% | 200% | 150% | 100% | 75% | 50% | 25%

Default 100%

Procedural alerts If you choose a map scale so large that it exceeds the limitations of your browser, the map automatically scales down.

Related

- To change the scale of the current window temporarily (per window), see *Scale* on page 152 in the **View** menu, and *Scale Up* or *Scale Down* on page 153.
- Looking for *Fit Map to Window* or *Fit Window to Map*? See *Scale* on page 152 in the **View** menu.
- To view the object title at smaller scales, position the mouse pointer over the icon until an information box appears. (Assumes that *Show pop-up info* is on.)

Show pop-up info

Toggles whether an information box associated with an object or a line appears when you position the mouse pointer over an icon.

Table 10: Pop-up information for objects

Information	Real device	Virtual device	Package
Tag	YES	(blank)	YES
Title	YES	YES	YES
Icon	YES	YES	YES
Management	YES	YES ("virtual")	—
IP address	YES	(blank)	—
MAC address	YES	(blank)	—
Priority	YES	YES	highest device priority within

Table 11: Pop-up information for lines

Information
Line Alarm Type
From
To

Default Off (clear)

Underline locked objects

Toggles the underlining of locked objects within all map windows. Objects that are "locked" from a packaging status are shown with a blue line under the icon.

Typically, objects acquire locked status when they are packaged by a user. When an object is locked, Network Discovery does not package or unpackage it.

Default Off (clear)

Related

- To change whether locked objects are underlined temporarily (per window), see *Underline Locked Objects* on page 152.
- To unlock an object, see *Unlock* on page 162.

Confirm packaging commands

Toggles whether commands that affect packaging present a dialog box asking you to confirm your action.

Effects The following commands are affected:

- *Layout* on page 150
- *Pack* on page 150
- *Unpack* on page 151
- *Unpack All* on page 151
- *Unpackage* on page 163

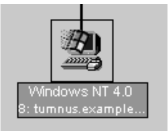
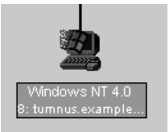
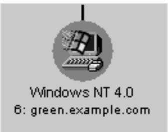
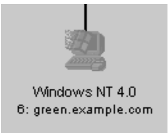
Default On (checked)

Shade icons when selected

There are two methods of indicating:

- selected icons
- “not seen” objects

Table 12: Shaded and non-shaded icons

Icon is...	Not shaded (default)	Shaded
Selected		
Not seen		

Shading icons is more intuitive, but it also requires more memory.

Limits Not available to Windows 95 or Windows 98 management workstations.

Default Off (clear)

Show icons when dragging

Selects how groups of objects are displayed when being moved.

Note: This setting has no effect on groups when they are not in motion.

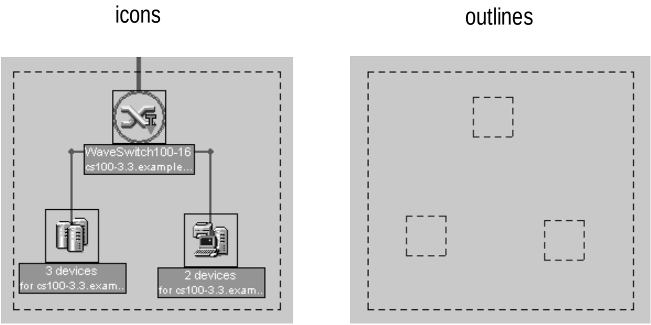
Note: This setting has no effect on single objects.

When to use it To ensure that a group is dragged smoothly and without flickering images, such as:

- when using a slow computer or video card
- when moving large groups of objects in a densely populated map

Options On (show icons) | Off (show outlines)

Figure 10-3: Icon group options



Default On (checked)

Open Health Panel with Network Map

Note: This setting does not affect the Aggregate Health Panel.

Causes the single-appliance Health Panel to be opened automatically whenever you click the **Network Map** button.

Use brief Health Panel

Note: This setting affects both the single-appliance Health Panel and the Aggregate Health Panel.

The Health Panel has two different views, detailed and brief. Detailed is the full Health Panel. This toggles the view you see when you start a map session.

⬆ ⬇ You can switch views at any time by using the arrow button in the bottom right corner of the Health Panel. This setting affects only which view you see initially.

Default Off (clear)

Related To switch between views temporarily, see *Switch view* on page 74.

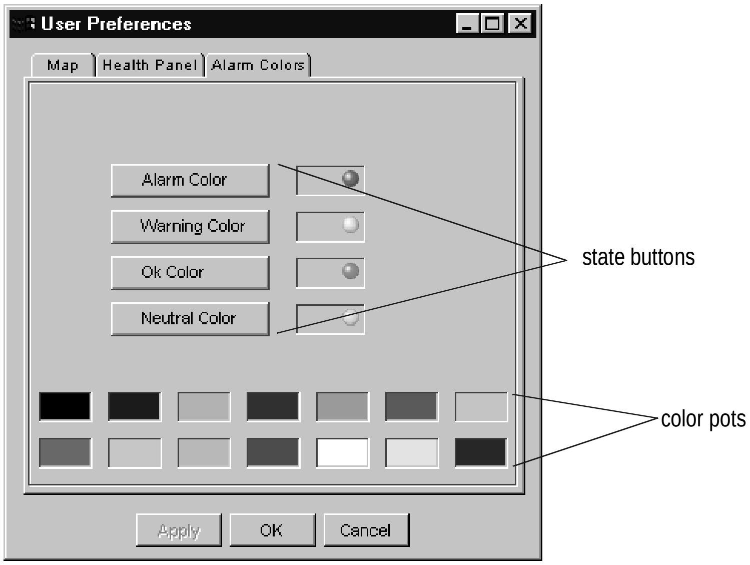
Alarm Colors

Selects colors used to indicate the alarm state of devices, ports, and lines.

Table 13: Alarm colors

Color	Association (default)	Customize
Black	group selection box	—
	Neutral (lines)	YES
Blue	locked object underline	—
Cyan	—	—
Dark Gray	—	—
Medium Gray	“not seen” background	—
Green	OK	YES
Light Gray	Neutral (devices)	YES
Purple	“located” box	—
Orange	—	—
Pink	—	—
Red	Alarm	YES
White	—	—
Yellow	Warning	YES
Maroon	—	—

Figure 10-4: Alarms dialog box



Options

- *state:* Alarm Color | Warning Color | Ok Color | Neutral Color
- *colors:* 14

Limits

Time to apply: up to 40 seconds

Default

Table 14: Default colors

State	Color
Alarm	Red
Warning	Yellow
OK	Green
Neutral (devices)	Light Gray
Neutral (lines)	Black

View

Most commands in this menu act on the map window (rather than the map session or map configuration).

- *Layout* on page 150
- *Pack* on page 150
- *Unpack* on page 151 or *Unpack All* on page 151
- *Create Package* on page 152
- *Underline Locked Objects* on page 152
- *Scale* on page 152
- *Scale Up* on page 153
- *Scale Down* on page 153
- *Fit Map to Window* on page 153
- *Fit Window to Map* on page 154

Limits

Maximum map windows: 10

Default

The default window size is two-thirds the size of the available desktop. The exact size depends on your screen resolution.

Related

- For a right-click **View** menu, see *Background* on page 171.
- To control the top object in a window, see *Properties* on page 159.

Layout

Reorganizes the layout of the active map window, then redraws the window.

When to use it

To tidy a map with confusing layout and crisscrossing connections.

Effects

- Destroys any custom layout.
- Clears fixed objects for the window—see *Position* on page 118.
- Does not destroy packages or change contents of packages.

Procedural alerts

You may be prompted to confirm this action—see *Confirm packaging commands* on page 146.

Related

- To move objects, see the *User Guide.*
- To move groups of objects, see the *User Guide.*

Pack

Automatically packages the active map window; that is, creates a package for each group of devices attached to the top device.

When to use it

To organize a map window.

Effects

- May create new packages.
- Does not "uncreate" or change current packages.

Limits

- The top device is not packaged.
- Only the active map window is packaged.

Procedural alerts

You may be prompted to confirm this action—see *Confirm packaging commands* on page 146.

Related

- To create a single package containing selected objects, see *Package* on page 164.
- To create an empty package, see *Create Package* on page 152.

Unpack

Note: In the Network Map window, this command is replaced by **Unpack All**.

Moves the contents of the active package window up one level.

Does not destroy any packages within the active window.

Effects

- Only the current package window is destroyed. Packages within the current package are not destroyed.
- Unlocks all objects.
- End node packages that were within the window are repackaged.

Procedural alerts

You may be prompted to confirm this action—see *Confirm packaging commands* on page 146.

Related

- See also *Unpack All* on page 151.
- To destroy a single package, see *Unpackage* on page 163.

Unpack All

Note: In a package window, this command is replaced by **Unpack**.

Unpackages the entire Network Map; that is, destroys all packages in all map windows. Then recreates end node packages.

When to use it

- To remove all packaging.
- To create a map window with minimum packaging.

Effects

- All packages are destroyed.
- Unlocks all objects.
- End node packages are repackaged.

Procedural alerts

You may be prompted to confirm this action—see *Confirm packaging commands* on page 146.

Related

See also *Unpack* on page 151.

Create Package

Creates an empty package with the title “New Package”.

Note: You cannot open an empty package. You must place at least one object in a package before you can open it.

Limits

You can create only one empty package per map window. If you try to create a second empty package, Network Discovery highlights the existing New Package.

Related

- To create a package that contains objects, see *Package* on page 164.
- To add objects to a New Package, either drag the New Package on top of an object, or drag an object on top of the New Package.
- To destroy a package, see *Unpackage* on page 163.
- Right-click: You can also find **Create Package** on right-click menus for the background of the map.

Underline Locked Objects

Toggles the underlining of locked objects within the active map window. Objects that are “locked” from a packaging status are shown with a blue line under the icon.

Typically, objects become locked when packaged by a user. When an object is locked, Network Discovery does not package or unpackage it.

Related

To change the default setting for all map windows, see *Underline locked objects* on page 145 in *User Preferences….*

Scale

Changes the scale at which icons are drawn. Affects the active map window only, not all map windows.

Changes the scale absolutely, not relative to the current scale. For relative change, see *Scale Up* on page 153 and *Scale Down* on page 153.

When to use it

- To get an overview of the map window, decrease the scale.
- To view a section of the map window, increase the scale.
- To create space in which to rearrange groups of objects, decrease the scale.
- To increase the legibility of object titles for projected presentations or for large printed maps, increase the scale. (To print a map, see *Page Setup* on page 134 and *Print…* on page 135.)

Effects

Changing **Scale** affects Print Range—see *Page Setup* on page 134.

Options

300% | 200% | 150% | 100% | 75% | 50% | 25%

Limits

If you choose a map scale so large that it exceeds the limitations of your browser’s memory, the map window automatically scales down.

Default

- *initial:* 100%
- *subsequent:* from **Scale** setting

Related

- To change the default scale for all map windows, see *Scale* on page 144.
- To change to the next larger or smaller scale, see *Scale Up* on page 153 or *Scale Down* on page 153.
- To change the scale to fit the window, see *Fit Map to Window* on page 153.
- To keep the scale the same but change the window size, see *Fit Window to Map* on page 154.
- To view the object title at smaller scales, position the mouse pointer over the icon until an information box appears. (Assumes that *Show pop-up info* is on.)

Scale Up

Changes the scale at which icons are drawn in the current map window. Selects the next largest scale value; that is, changes the scale of the current window relative to the current scale.

Effects Changing **Scale** affects Print Range—see *Page Setup* on page 134.

Limits Not available if the current scale is 300%.

Related Right-click: You can also find **Scale Up** on right-click menus for the background of the map.

Scale Down

Changes the scale at which icons are drawn in the current map window. Selects the next smallest scale value; that is, changes the scale of the current window relative to the current scale.

Effects Changing **Scale** affects Print Range—see *Page Setup* on page 134.

Limits Not available if the current scale is 25%.

Related Right-click: You can also find **Scale Down** on right-click menus for the background of the map.

Fit Map to Window

Adjusts the scale of your map to fit the current open window.

May cause the scale to be set to a value not available through the menu (for example, 28%).

When to use it

- When your map will not fit in the current window (even at a scale of 25%). The scale will be decreased.
- When there is a lot of blank space on the map—that is, a few objects are clustered in a small section of a large window—and you want to see the objects clearly. The scale will be increased, but the map window will remain the same size.

Effects

Changing **Scale** affects Print Range—see *Page Setup* on page 134.

Related

Right-click: You can also find **Fit Map to Window** on right-click menus for the background of the map.

Fit Window to Map

Adjusts the size of your window to accommodate the scale of your map.

When to use it

- When there is a lot of blank space, and you want to use the space on your screen for other windows. The current map window will be smaller.
- When the map won't fit into the current window at the current scale. The current map window will be larger (possibly larger than the screen).

Effects

Changing **Scale** affects Print Range—see *Page Setup* on page 134.

Related

Right-click: You can also find **Fit Window to Map** on right-click menus for the background of the map.

Object

Provides commands for devices and packages. You must select an object in order for the menu to be made active.

Not all commands are available to all types of objects.

Table 15: Object menu commands available by object type

	Device		Package	
Command	IP address	MAC address *or* virtual	not empty	empty
Open	[multiple]	[multiple]	[multiple]	—
Analyze Services	[single]	[single]	—	—
Web	[single]	—	—	—
Telnet	[single]	—	—	—
Manage*	[single]	—	—	—
IP Ping	[single]	—	—	—
SNMP Ping	[single]	—	—	—
Traceroute	[single]	—	—	—
Browse MIB	[single]	—	—	—
Properties	[single]	[single]	[single]	—
Lock	[multiple]	[multiple]	[multiple]	—
Unlock	[multiple]	[multiple]	[multiple]	—
Reset MTTR and MTBF [Administrator or IT Manager only]	[multiple]	[multiple]	[multiple]†	—
Purge [Administrator or IT Manager only]	[multiple]	[multiple]	[multiple]	—
Unpackage	—	—	[single]	[single]
Package	[multiple]	[multiple]	[multiple]	—
Promote‡	[multiple]	[multiple]	[multiple]	[single]

* This is the default name for this command. The command name displayed depends on the settings for *The screen shows the current settings. The default is to package all classes, and to create the generic End Node class last.* on page 373.
† Applied to entire contents of package (recursively).
‡ Not available in the Network Map window.
[single] = available to single objects
[multiple] = available to single and multiple objects

- For a right-click **Object** menu for devices, see *Device* on page 170.
- For an abbreviated right-click **Object** menu for packages, see *Package* on page 170.
- For an abbreviated right-click **Object** menu for multiple objects, see *Multiple objects* on page 170.

Open

Device: Opens a Device Manager window for the device.

Package: Opens (or brings forward) the package window.

Limits

- *maximum package windows:* 10
- Not available to empty packages (for example, "New Package").

Related

- To close a package window, click the window's close box.
- To open a map configuration, see *Open…* on page 131.
- Alternative: You can also double-click an icon to open a device or package.
- Right-click: You can also find **Open** on right-click menus for devices, packages, and lines.

Analyze Services

Opens the Service Analyzer query window with the current device already selected as Device 1. Enables the user to view the state of the path between this device and any other device on the Network Map. See also *Chapter 15, Service Analyzer*.

Web

Attempts to open a web browser window for the device.

When to use it

If the device supports web-based management or other web services.

Limits

- The device must have an IP address. If not, this command is dimmed.
- The device must support HTTP sessions. (Network Discovery may try and not succeed.)

Related

To control how HTTP connections are made, see *Appliance Proxy Services* on page 358.

Note: *for Aggregator*—See also **Administration** > **Remote appliance administration** > **Remote appliance properties** (*Remote Appliance Properties* on page 327)

Telnet

Attempts to open a Telnet session. Many network devices provide Telnet as a means to set up and configure the device.

Limits

- The device must have an IP address. If not, this command is dimmed.
- The device must support Telnet sessions. (Network Discovery may try and not succeed.)

Related

To control how Telnet connections are made, see *Appliance Proxy Services* on page 358.

Note: *for Aggregator*—See also Administration > **Remote appliance administration** > **Remote appliance properties** (*Remote Appliance Properties* on page 327)

Manage

Launches an element manager of your choice.

Note: This is the default name for this command. The command name displayed depends on the settings for *Element Management* on page 374.

Limits

- The device must have an IP address. If not, this command is dimmed. For example, you cannot manage a virtual device.
- The URL must be defined in *The screen shows the current settings. The default is to package all classes, and to create the generic End Node class last.* on page 373. If not, this command is dimmed.

Procedural alerts

Note: *for Netscape*—The first time you manage through an executable, you will be asked to grant permission.

Related

To define the URL that *Manage* will launch, see *The screen shows the current settings. The default is to package all classes, and to create the generic End Node class last.* on page 373.

IP Ping

Pings the device to see if it responds, and how quickly.

Limits

The device must have an IP address. If not, this command is dimmed.

Default

5 pings

SNMP Ping

Queries the device for basic SNMP information and displays this information.

Limits

- The device must have an IP address.
- The device must support basic SNMP functionality.

Default

Community string

- Demo, IT Employee, IT Manager: “public”
- Administrator: the read community string for the device as defined in **Administration** > **Network configuration** > **Community Property Groups**.

Traceroute

Displays the path that data takes to get from the Peregrine appliance to the selected device by listing the routing devices associated with each hop of the journey. The device identifier is often the domain name, where available, but can also be the IP address. Each device title is hyperlinked to a Device Manager.

Traceroute also displays the amount of time each hop took. This time is the round trip in milliseconds. Traceroute includes two retry hops for each try, so the times for all three hops are shown.

Traceroute helps you to understand where on the network problems are occurring. It is often used after *IP Ping* on page 157 has been used to confirm the existence of a device.

Note: The path displayed by traceroute is at OSI layer 3 and may not match the connectivity on the Network Map or in the *Service Analyzer* on page 251.

When to use it

- If you suspect that you are losing packets due to a large hop count.

  In a TCP/IP network, where data are transmitted in packets, the header for a packet tracks the hop count. If the hop count grows too large, the packet is discarded.
- If you are trying to determine the point along the path where traffic is slowing down or getting lost altogether.
- If you are trying to determine the precise path taken—not so much to solve a problem as for general information.
- To confirm that your routers are included in IPv4 address ranges set up for discovery in **Administration** > **Network configuration** > **Add IPv4 ranges** (*Network Configuration* on page 317

Output

Results of an asterisk for the device and for all three times (that is the result * * * *) indicates that data is not available for that hop of the journey, and usually indicates a trouble spot along the path.

Table 16: Traceroute special results

Chars.	Meaning
*	no response within a 3-second timeout interval
!	ttl <= 1*
!H	host is unreachable
!N	network is unreachable
!P	protocol is unreachable
!S	source route failed
!F	fragmentation needed
!X	communication is prohibited administratively
!V	a host precedence violation has occurred
!C	precedence cutoff is in effect

* The ttl value is supposed to start at 1 and increase by 1 until the host is reached.

Related To see the OSI layer 2 path between any two devices, see also *Analyze Services* on page 156.

Browse MIB

Opens the MIB Browser to allow the user to view the device's SNMP MIB. See also *Chapter 17, MIB Browser*.

Administrator or IT Manager: The MIB Browser also allows an experienced user of an Administrator or IT Manager account to manipulate the device on a more detailed level.

Limits

- The device must have an IP address. If not, this command is dimmed.
- The device must support basic SNMP functionality. (Network Discovery may try and not succeed.)

Properties

Modifies properties of an object. Properties affect an object's appearance, priority, and placement within a map window.

Tip: To have changes to a device's properties (other than icon) reflected when you open a Device Manager for the object, you must save your map configuration. See *Save* on page 132 or *Save As…* on page 132.

Administrator or IT Manager: Device icons can only be changed by an Administrator or IT Manager account.

Effects

- Changing a device icon:
  - affects device type
  - can affect priority
  - can affect events notification and logging
  - can affect packaging

Warning: Changing a device icon always affects the configurations of all accounts and event filters, even if **Save As Prime** [Administrator or IT Manager only] is not used. Changes take effect almost *immediately* (at the beginning of the next poll cycle).

- Changing the top object in a window causes the window to issue the command *Layout* on page 150.

Options

Table 17: Object properties

Property	Object type	Notes
Icon	device	Administrator or IT Manager accounts only
	package	all accounts
Title	device, package	Administrator or IT Manager: Prime map configuration affects other account
Priority	device only	—
Top of Network	device, package	—

Limits

- Available to single icons. Not available to an empty package.
- *Icons:* see Figure 10-5 and Figure 10-6 on page 161
- *Titles:* input: 1–80 characters; display: 1–20 characters; valid characters: A–Z, a–z, 0–9, *(space), (most punctuation, excluding* ' *[single quote] and* " *[double quote])*
- *Priority:* 1–6; see *Priority* on page 28 and *Priority* on page 118
- *Time to take effect (device icons):* several minutes, depending on your network's poll cycle

Figure 10-5: Device icons

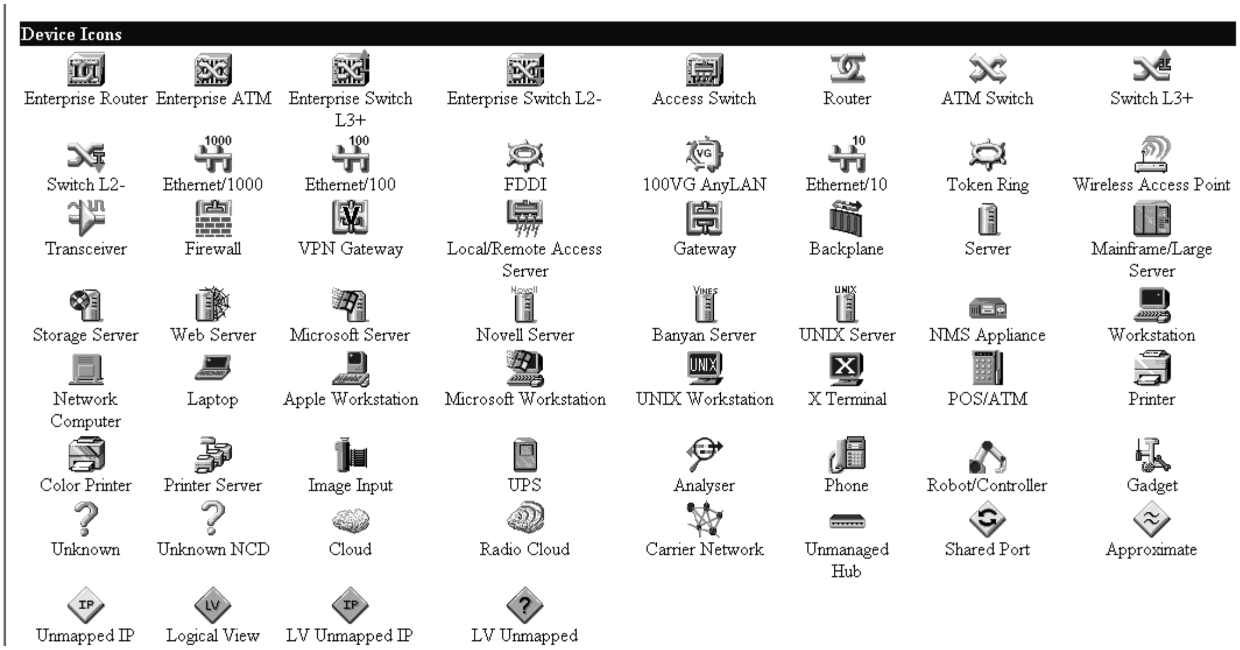
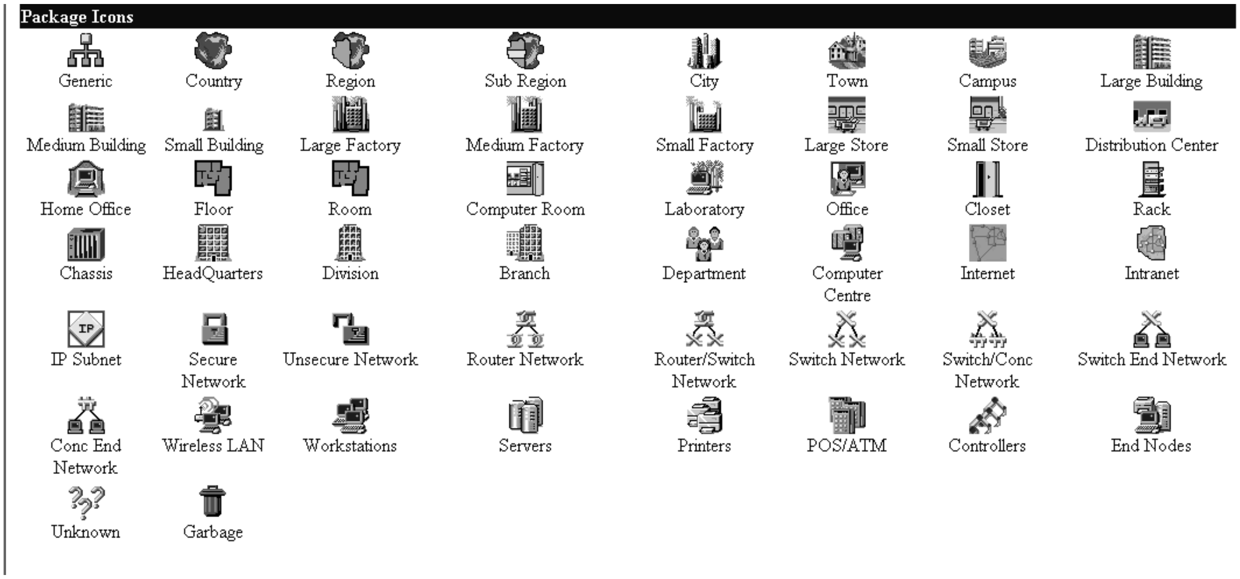


Figure 10-6: Package icons



Related Right-click: You can also find **Properties** on the right-click menus for devices and packages.

Lock

Sets the packaging status of an object to locked.

As a result, Network Discovery does not automatically:

- package the object
- unpackage the object
- destroy the packaging containing the object

The user is still able to package and unpackage the object.

The following commands automatically apply locked status to an object:

- *Unpackage* on page 163
- *Package* on page 164
- *Promote* on page 164

Note: When objects are promoted into the Network Map, they may be unlocked.

When to use it To prevent automatic packaging of an object.

Limits Available to unlocked objects.

Related To view the lock status of an object, see *Underline locked objects* on page 145 in *User Preferences…* or see *Underline Locked Objects* on page 152.

Unlock

Sets the packaging status of an object to unlocked. As a result, Network Discovery can automatically adjust its packaging. (All objects have a packaging status. They are either locked or unlocked. By default, objects are unlocked.)

The following command automatically applies unlocked status to an object:

- *Unpack All* on page 151

Note: When objects are promoted into the Network Map, they may be unlocked.

When to use it

To allow automatic packaging of an object.

Limits

Available to locked objects.

Related

To view the lock status of an object, see *Underline locked objects* on page 145 in *User Preferences…* or see *Underline Locked Objects* on page 152.

Reset MTTR and MTBF [*Administrator or IT Manager only*]

Resets the values for Mean Time To Repair (MTTR) and Mean Time Between Failures (MTBF) for the device.

Warning: Changing a device icon always affects the configurations of all accounts, even if **Save As Prime** [Administrator or IT Manager only] is not used. Changes take effect *immediately*.

When to use it

- When a device has been replaced
- When a device has been upgraded, and is therefore faster to repair
- Whenever past behavior of a device is no longer relevant

Limits

- Available to any combination of single and multiple devices and packages.
- Not available when using the **Forecast** command to view the Network Map.

Related

Right-click: You can also find **Reset MTTR and MTBF** [Administrator or IT Manager only] on right-click menus for packages and multiple objects.

Purge *[Administrator or IT Manager only]*

Removes a device from the Network Map.

Warning: This action cannot be undone.

Warning: Purging a device always affects the configurations of all accounts, even if **Save As Prime** [Administrator or IT Manager] is not used.

Important: You are *not* making a physical change to the device or network. If you purge a device but the device is still present in your network and still operational, Network Discovery will rediscover the device and the device will reappear on the Network Map. To prevent the device from reappearing, you must actually disconnect the device from your network, or you must apply to the device a Network Property Group or Set with the property, "Allow devices" set to "Off" (**Administration** > **Network Configuration** > **Network Property Groups**—see *Network Configuration* on page 317).

If a device has not been seen for the period set (in **Administration** > **Network Tuning** > **Expiry** > **Device Purge Intervals**—see *Expiry* on page 352), Network Discovery automatically purges it.

When to use it

When a device has been removed from the network and you wish to update the Network Map.

Effects

- Deletes the statistical history associated with the device. This in turn affects the graphs and reports for this device.
- Deletes the events associated with the device from the event log.

Limits

- Available to any combination of single and multiple devices and packages.
- Not available when using the **Forecast** command to view the Network Map.
- *Time to take effect:* start of the next poll cycle

Related

- To adjust how long Network Discovery waits before automatically purging a device, see Device Purge Intervals in *Expiry* on page 352.
- You can also purge a device by using the Device Manager—see *Purge device [Administrator or IT Manager only]* on page 202.
- To purge a port, see *Purge Port [Administrator or IT Manager only]* on page 226.
- To purge an attribute, see *Purge Attribute [Administrator or IT Manager only]* on page 246.
- Right-click: You can also find **Purge** [Administrator or IT Manager only] on right-click menus for packages and multiple objects.

Unpackage

Non-empty packages: Causes the selected package to be unpackaged, which also deletes the package.

Empty packages: Deletes the package.

Effects

Locks all objects within the package (unless they are unpackaged into the Network Map).

Limits

Available to single packages only.

Procedural alerts

You may be prompted to confirm this action—see *Confirm packaging commands* on page 146.

Related

- To create a package, see *Package* on page 164 and *Create Package* on page 152.
- To automatically create packages, see *Pack* on page 150.
- To delete all packages, see *Unpack* on page 151.
- Right-click: You can also find **Unpackage** on right-click menu for packages.

Package

Creates a package, then places all selected objects into the package.

Effects Locks all selected objects.

Limits Not available to an empty package.

Related

- To create an empty package, see *Create Package* on page 152
- To automatically create packages, see *Pack* on page 150.
- To remove objects from a package, see *Unpackage* on page 163 and *Promote* on page 164.
- Right-click: You can also find **Package** on right-click menus for packages and multiple objects.

Promote

Moves the objects to the window above the current window. (In terms of hierarchy, not screen space.)

Empty package: Deletes the package.

Effects

- When the last object is promoted out of the package, the package is destroyed.
- Locks all selected objects (unless they are promoted into the Network Map).

Limits Not available in the Network Map window.

Related

- Alternative: Drag the icon to the “Up a Level” icon (package windows only).
- Right-click: You can also find **Promote** on right-click menus for packages and multiple objects.

Tools

This menu provides:

- the same functions as the main Toolbar
- the Health Panel reports
- a shortcut to *Network Exceptions* on page 167
- a shortcut to *Appliance* on page 167
- *Forecast* on page 168

Aggregate Health Panel

Opens the Aggregate Health Panel—see *Chapter 6, Aggregate Health Panel*.

Note: *for Aggregator*—Available only when an Aggregator license is present.

Aggregate Events Browser

Opens the Aggregate Events Browser—see *Aggregate Events Browser* on page 262.

Note: *for Aggregator*—Available only when an Aggregator license is present.

List Remote Appliances

Lists the remote appliances—see *Chapter 8, Remote Appliances*.

Note: *for Aggregator*—Available only when an Aggregator license is present.

Health Panel

Opens the Health Panel, or makes an opened Health Panel the front-most window. See *Chapter 5, Health Panel*.

Network Map

- If the Network Map window is closed, this command opens it.
- If the Network Map is open, this command makes it the front-most window.

Related To close the Network Map window, see *Close* on page 138.

Service Analyzer

Opens the Service Analyzer—see *Chapter 15, Service Analyzer*.

Events Browser

Opens the Events Browser—see *Chapter 16, Events Browser*.

Find…

Searches for devices and ports of devices—see *Chapter 17, Find*.

Shortcut Press Control-F to launch the Find tool.

Home

Displays the Network Discovery Home page in your web browser—see *Home* on page 40.

Status

Opens the Status menu.

Reports

Opens the Reports menu—see *Chapter 18, Reports*.

Administration

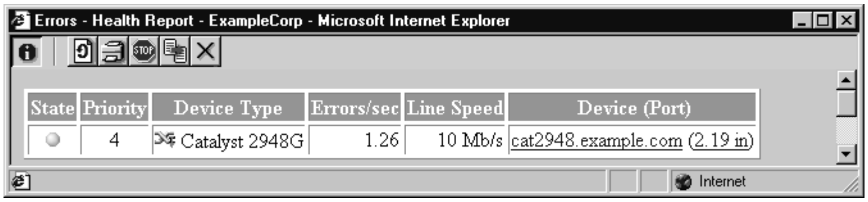
Opens an Administration menu related to your account type.

- Demo—the Administration menu is not available
- IT Employee and IT Manager—see *Administration for IT Employee and IT Manager Accounts* on page 281. With respect to the Administration menu, an IT Manager account has capabilities similar to an IT Employee account. It is only with respect to the Network Map that an IT Manager account is similar to an Administrator account.
- Administrator—see *Administration for Administrator Accounts* on page 291

Health Panel Reports

All reports provide one row of data for each alarm or warning.

Figure 10-7: Sample Health Panel report



Errors - Health Report - ExampleCorp - Microsoft Internet Explorer

State	Priority	Device Type	Errors/sec	Line Speed	Device (Port)
○	4	Catalyst 2948G	1.26	10 Mb/s	cat2948.example.com (2.19 in)

The rows are sorted by state, by priority, and by value. The rows of a Line Faults report have two extra columns for data not meaningful in a Device Faults report.

Table 18: Data reported in a Health Panel report

Column	Line	Device	Notes
State	YES	YES	alarm | warning | ok
Priority	YES	YES	1–6
Value	YES	YES	see Table on page 10-166
Line speed	YES	—	in Gb/sec., Mb/sec., kb/s, or b/s
Device	YES	YES	hyperlinked to Device Manager

Table 18: Data reported in a Health Panel report

Column	Line	Device	Notes
Port	YES	—	hyperlinked to Port Manager
Current Connection (Port)	—	YES	Changes report only
Previous Connection (Port)	—	YES	Changes report only

Table 19: Values for a Health Panel report

Category	Value
Line Breaks	Broken since (time/date)
Utilization	Utilization (%)
Delay	Response time (milliseconds)
Collisions	Collisions/sec.
Broadcasts	Frames/sec.
Errors	Frames/sec.
Device Breaks	Broken since (time/date)
Packet Loss	Unicasts formula (%)
Changes	■ Was added at (time/date) ■ Last moved (time/date) ■ Last seen at (time/date)
NEWS	Days until
MTTR	MTTR (hours)
MTBF	MTBF (days)

When to use it

- If you prefer tabular data over a graphic representation.
- When you want to have a static display of alarms or warnings at a given moment.
- To view all line alarms and warnings, including those that have no line or icon in the Network Map.

Limits

No faults affecting devices below the *Priority List* on page 72 are displayed.

Related

- These reports are also available from the Health Panel—see *Reports* on page 69.
- Health Panel reports have a special right-click menu.

Network Exceptions

Provides a shortcut to a summary of Network Exceptions (see *Support Reports* on page 276).

Appliance

Provides a shortcut to **Status** > **Appliance Health**.

Forecast

Predicts how the network will perform in the future.

Network Discovery computes a probable view of the Network Map based on existing data. Network Discovery assumes that no physical changes will be made to the network. Predictions are made based on the peak busy minute per week, and use linear trends with some data cleaning.

Predictions have three grades of confidence: high, medium, and low. The longer Network Discovery has been running, the more confidence it has in its predictions. Network Discovery is usually most confident about the near future, and less confident about the distant future.

Confidence is based on the number of complete months of network history in the Network Discovery database. (Clearing the database resets the history.)

Table 20: Confidence of Forecast predictions

Confidence	Determining factor
Low	number of months from now > number of months of history accumulated
Medium	3 times number of months from now > number of months of history accumulated
High	3 times number of months from now <= the number of months of history accumulated

Note: The map is always returned to the present when you *Close Map* on page 138.

Effects

- The progress bar on the Health Panel or the map window’s status bar becomes static and displays the Forecast view instead. Example: “+ 2 months”
- The following commands are disabled:

Table 21: Map menu items disabled by Forecast

Menu	Command
File	New
	Open…
	Open Copy of Prime
	Save
	Save As…
	Save As Prime [Administrator or IT Manager only]
Object	Reset MTTR and MTBF [Administrator or IT Managerr only]
	Purge [Administrator or IT Managerr only]

Procedural alerts

To return to the present, select “0 months”.

Help

Gives two choices, **Network Discovery Help** and **About Network Discovery**. The Network Discovery Help page is the same page that opens from the Toolbar **Help** button. For information on the Network Discovery Help page, see *Help* on page 40, in Chapter 3, *The Toolbar and Other Navigation*.

About Network Discovery

Information about the makers of and modules within Network Discovery. Displayed at the top of the page is the Network Discovery version number.

Ways of opening

- Available as a separate pull-down menu item from the Help button in the Health Panel, in any Network Map window and in the MIB Browser.
- Also available from the Network Discovery Help page.

Related

- For module version numbers, see **Status** > **Current Settings** > **Installed Components.**
- For licenses, see **Status** > **Current Settings** > **Installed Licenses.**

Procedural Alert

The help button in the top right hand corner of the About page leads to information about your browser.

Right-click Menus

There are five right-click menus available from map windows. Network Discovery selects the appropriate right-click menu based on where the mouse pointer is positioned.

Device

When you point at a single device, clicking the right-most button on your mouse selects the device and displays an abbreviated **Object** menu—only the **Unpackage** command will be missing.

Note: *for Aggregator*—When the device is a Peregrine appliance, a **Remote Appliance** sub-menu is available. The following **Tools** menu commands are available from this sub-menu:

- *Health Panel* on page 165
- *Network Map* on page 165
- *Service Analyzer* on page 165
- *Events Browser* on page 165
- *Find…* on page 165

Package

When you point at a single package, clicking the right-most button on your mouse selects the package and display an abbreviated **Object** menu that includes the following commands:

- *Open* on page 156
- *Properties* on page 159
- *Lock* on page 161
- *Unlock* on page 162
- *Reset MTTR and MTBF [Administrator or IT Manager only]* on page 162
- *Purge [Administrator or IT Manager only]* on page 162
- *Unpackage* on page 163
- *Package* on page 164
- *Promote* on page 164

Multiple objects

When you point at multiple selected objects, clicking the right-most button on your mouse displays an abbreviated **Object** menu that includes the following commands:

- *Open* on page 156
- *Lock* on page 161
- *Unlock* on page 162
- *Reset MTTR and MTBF [Administrator or IT Manager only]* on page 162
- *Purge [Administrator or IT Manager only]* on page 162

- *Package* on page 164
- *Promote* on page 164

Line

When you point at a line, clicking the right-most button on your mouse displays a menu that contains just the *Open* command.

Invoking this right-click menu causes any selected objects to be deselected.

Background

When you point at an area of the map that does not contain any objects or lines, clicking the right-most button on your mouse displays an abbreviated **View** menu that includes the following commands:

- *Layout* on page 150
- *Create Package* on page 152
- *Underline Locked Objects* on page 152
- *Scale Up* on page 153
- *Scale Down* on page 153
- *Fit Map to Window* on page 153
- *Fit Window to Map* on page 154
- *Close* on page 138

Invoking this right-click menu causes any selected objects to be deselected.

11 Device Manager

CHAPTER

- To explore icon buttons in the toolbar menus:
  - Manager toolbar (page 174)
  - Statistics toolbar (page 184)
  - Events toolbar (page 190)
- To interpret data in the Device Manager window, see *Panel Elements* on page 207.

Introduction

Provides you with detailed information about a device, in one of several panels.

Ways of opening

- From a map window, double-click a device icon.
- From a map window, right-click the device icon and click **Open**.
- From a map window, click a device icon. From the **Object** menu, click **Open**.
- From a map window, the Health Panel, or a Health Panel report: From the **Tools** menu, click Find. Enter a device address or title, then click **Find**.
- From a Service Analyzer path diagram, click a device icon.
- From the Toolbar, click the **Find** button. Enter a device address or title, then click **Find**.
- Click a hyperlinked device title. (Hyperlinked devices appear in Managers panels, in the Events Browser, in reports, and in **Network Map Sessions** status.)

Default panel

- *initial:* State
- *subsequent:* from *Account Properties* on page 282

Toolbar

Availability of buttons in the Device Manager toolbar.

Table 1: Available toolbar buttons

Icon	Button name	Page	No IP address	Not in database	Not on Network Map or Unknown	Virtual device	Demo or IT Employee user
i	Configuration	page 175	YES	—	YES	YES	YES
!	State	page 182	YES	—	YES	—	YES
Σ	Statistics	page 184	YES	—	YES	—	YES
	Ports	page 186	YES	—	YES	YES	YES
	Events	page 190	YES	—	YES	—	YES
	Diagnosis	page 192	YES	—	YES	YES	YES
	Buttons on the Diagnosis Panel						
	i (Diagnosis) Configuration	page 192	YES	—	YES	YES	YES
	IP •))) IP Ping	page 196	—	YES	YES	—	YES
	TRACE •))) Traceroute	page 196	—	YES	YES	—	YES
	SNMP •))) SNMP Ping	page 197	—	YES	YES	—	YES
	DNS •))) DNS Query	page 198	—	YES	YES	—	YES
	Locate	page 198	YES	—	—	YES	YES
	Service Analyzer	page 198	YES	—	—	YES	YES
	Manage	page 199	—	YES	YES	—	YES
	Browse MIB	page 199	—	YES	YES	—	YES
	View Scan Data		YES	NO	NO	NO	YES
	Web	page 200	—	YES	YES	—	YES
	Telnet	page 201	—	YES	YES	—	YES

Table 1: Available toolbar buttons (Continued)

Icon	Button name	Page	No IP address	Not in database	Not on Network Map or Unknown	Virtual device	Demo or IT Employee user
	Update Model	page 202	—	YES	YES	—	—
	Purge Device	page 202	YES	NO	—	YES	NO
	Properties	page 204	YES	YES	—	YES	YES
	Refresh	page 206	YES	YES	YES	YES	YES
	Print	page 206	YES	YES	YES	YES	YES
	Text	page 206	YES	YES	YES	YES	YES
	Close	page 206	YES	YES	YES	YES	YES

Configuration

Identifies a device and presents an overview of the device’s identity, position, and status.

Limits

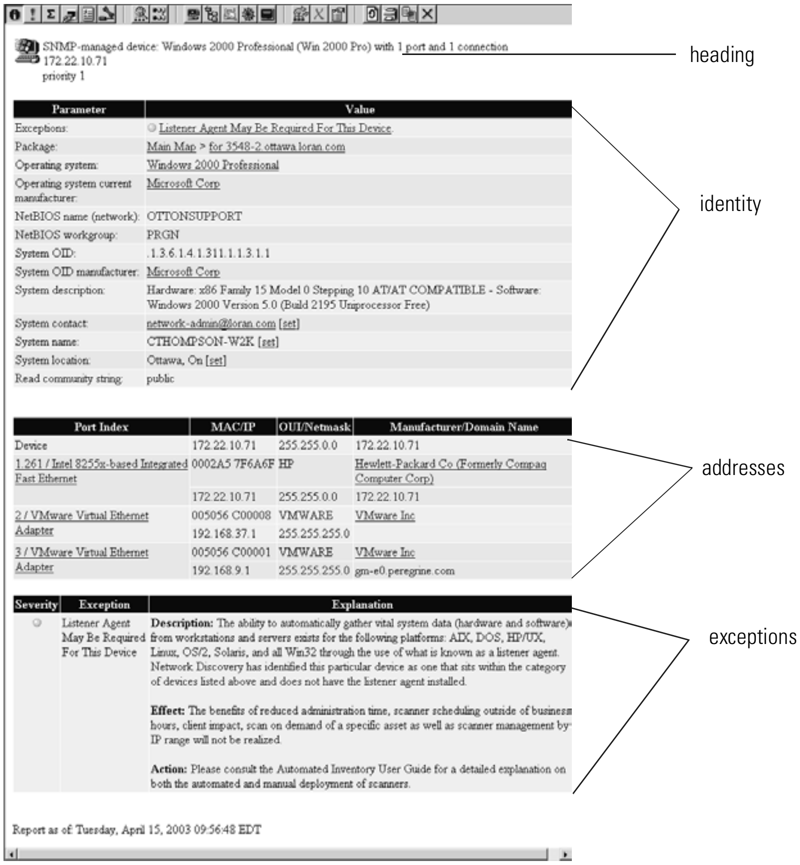
This panel is blank if the device is not in the Network Discovery database.

Details

This panel is divided into the following principal sections:

- Heading
- Identity table (real devices only)
- Address table (real devices only)
- Exceptions table (if relevant)

Figure 11-1: Sections of Configuration panel



SNMP-managed device: Windows 2000 Professional (Win 2000 Pro) with 1 port and 1 connection
172.22.10.71
priority 1

Parameter	Value
Exceptions:	○ Listener Agent May Be Required For This Device.
Package:	Main Map > for 3548-2.ottawa.loran.com
Operating system:	Windows 2000 Professional
Operating system current manufacturer:	Microsoft Corp
NetBIOS name (network):	OTTONSUPPORT
NetBIOS workgroup:	PRGN
System OID:	.1.3.6.1.4.1.311.1.1.3.1.1
System OID manufacturer:	Microsoft Corp
System description:	Hardware: x86 Family 15 Model 0 Stepping 10 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)
System contact:	network-admin@loran.com [set]
System name:	CTHOMPSON-W2K [set]
System location:	Ottawa, On [set]
Read community string:	public

Port Index	MAC/IP	OUI/Netmask	Manufacturer/Domain Name
Device	172.22.10.71	255.255.0.0	172.22.10.71
1.261 / Intel 8255x-based Integrated Fast Ethernet	0002A5 7F6A6F	HP	Hewlett-Packard Co (Formerly Compaq Computer Corp)
	172.22.10.71	255.255.0.0	172.22.10.71
2 / VMware Virtual Ethernet Adapter	005056 C00008	VMWARE	VMware Inc
	192.168.37.1	255.255.255.0	
3 / VMware Virtual Ethernet Adapter	005056 C00001	VMWARE	VMware Inc
	192.168.9.1	255.255.255.0	gm-e0.peregrine.com

Severity	Exception	Explanation
○	Listener Agent May Be Required For This Device	**Description:** The ability to automatically gather vital system data (hardware and software) from workstations and servers exists for the following platforms: AIX, DOS, HP/UX, Linux, OS/2, Solaris, and all Win32 through the use of what is known as a listener agent. Network Discovery has identified this particular device as one that sits within the category of devices listed above and does not have the listener agent installed. **Effect:** The benefits of reduced administration time, scanner scheduling outside of business hours, client impact, scan on demand of a specific asset as well as scanner management by IP range will not be realized. **Action:** Please consult the Automated Inventory User Guide for a detailed explanation on both the automated and manual deployment of scanners.

Report as of: Tuesday, April 15, 2003 09:56:48 EDT

Heading

The heading also appears in the State, Ports State, Ports Statistics, and Diagnosis panels (when available).

Table 2: Heading

Element	Notes	Type
Icon	for a complete list, see Figure 11-5 and Figure 11-6	all
Descriptive prefix	for example, “SNMP-managed device”	
Device type	for a complete list, see **Help** > **Device Types**	all
Device tag	see *Tag* on page 116	real
Virtual device map title	see *Virtual devices* on page 121	virtual
No. of ports	the number Network Discovery uses for the port may not match the physical port	all
No. of connections	includes user-assigned connections	all
Icon flag	appears if assigned by an Administrator or IT Manager account	
Object title	first title available; see *Title* on page 208	all

Table 2: Heading (Continued)

Element	Notes	Type
Address	IP address; does not appear if identical to object title	real
Title flag	appears if assigned by Prime configuration or user	all
Priority	see *Priority* on page 28	all
Priority flag	appears if assigned by a user	all
Virtual device number	created by Network Discovery or by an Administrator or IT Manager account	virtual

Identity

The information in this table can come from three sources: the Network Discovery Rulebase and the SNMP MIB of the object and, if you are using it, Peregrine's Express Inventory (the WMI collector). For information on setting up and using the WMI collector, see your ServiceCenter Essentials documentation.

The Rulebase determines the device's operating system, application, device family, and model. It determines as many of these as are available.

Some of the information collected from the SNMP MIB has been set by the device manufacturer; other information can be customized. For information on how to enter MIB data so that Network Discovery interprets it as a link, see *Special input syntax* on page 36 and *Appliance System Variables* on page 294.

More elements of identity appear for thePeregrine Appliance than for any other device.

Table 3: Elements of Identity table in Configuration panel

Data	Example	Optional	Creator	Administrator or IT Manager
Exceptions	—	YES	Network Discovery	—
Package	Main Map	YES—if you have not opened a map configuration since this object was discovered	Network Discovery/account	—
Family	Cisco 2600 Series Modular Access Routers	YES	Network Discovery Rulebase	—
Family current manufacturer	Cisco Systems Inc	YES	Network Discovery Rulebase	—
Model	Cisco 2621XM Modular Access router	YES	Network Discovery Rulebase	—
Model current manufacturer	Cisco Systems Inc	YES	Network Discovery Rulebase	—
Model historical manufacturer*	Cisco Systems Inc	YES	Network Discovery Rulebase	—

Table 3: Elements of Identity table in Configuration panel (Continued)

Data	Example	Optional	Creator	Administrator or IT Manager
Operating system	Cisco IOS Version 12.2 (8) T5	YES	Network Discovery Rulebase	—
Operating system current manufacturer	Cisco Systems Inc	YES	Network Discovery Rulebase	—
Operating system historical manufacturer	Cisco Systems Inc	YES	Network Discovery Rulebase	—
Network Function	—	YES	Network Discovery Rulebase	—
Network Function current manufacturer	—	YES	Network Discovery Rulebase	—
Network Function historical manufacturer	—	YES	Network Discovery Rulebase	—
Operating system	Linux	YES	Peregrine's Express Inventory (the WMI collector)	—
Service pack	—	YES	Peregrine's Express Inventory (the WMI collector)	—
NetBIOS name (network)	—	YES	device owner	—
NetBIOS workgroup	MARKETING	YES	device owner	—
rulebase extra info	—	—	Network Discovery Rulebase	—
Device-specific title	—	—	scripts	—
System OID	.1.3.6.1.4.1.295.5.1.1.2	—	manufacturer	—
System OID manufacturer	PlainTree Systems Inc	YES	Network Discovery Rulebase	—
System description	Ethernet Switch	—	manufacturer	—
System contact	system@example.com	—	device owner	set† link
System name	ws1216-2	—	device owner	set† link
System location	Server Room	—	device owner	set† link
Read community string	public	YES	device owner	view
Write community string	n/a	YES	device owner	view
Asset tag	78LL996	—	Peregrine's Express Inventory (the WMI collector)	—
BIOS asset tag	—	—	Peregrine's Express Inventory (the WMI collector)	—
BIOS product name	eserver xSeries 330 -[867441X]-	—	Peregrine's Express Inventory (the WMI collector)	—

Table 3: Elements of Identity table in Configuration panel (Continued)

Data	Example	Optional	Creator	Administrator or IT Manager
BIOS product manufacturer	IBM	—	Peregrine's Express Inventory (the WMI collector)	—
BIOS serial number	78LL996	—	Peregrine's Express Inventory (the WMI collector)	—
BIOS chassis	—	—	Peregrine's Express Inventory (the WMI collector)	—
CPU	Pentium III 1133 MHz (Genuine Intel)	—	Peregrine's Express Inventory (the WMI collector)	—
NetBIOS name (scan)‡**	DUPONT	YES	device owner	—
NetBIOS name (network)	DUPONT	YES	device owner	—
Last name	DUPONT	—	Peregrine's Express Inventory (the WMI collector)	—
first name	MARIE	—	Peregrine's Express Inventory (the WMI collector)	—
Memory (MB)	1024	—	Peregrine's Express Inventory (the WMI collector)	—
Windows/NIS domain	—	—	Peregrine's Express Inventory (the WMI collector)	—

* Appears only when different from the current manufacturer.
† A shortcut to the MIB Browser.
‡ On Windows workstations, frequently the same as the system name.
** NetBIOS data is blank unless the device has an IP address.

Package:

- Displays the position of a device within the packaging of the Network Map. Click on a hyperlink to open a corresponding map window.
- If you have a map open, this row reflects the packaging of your current configuration. If you open the Device Manager and then make packaging changes that affect the device, click the **Refresh** button to have this row updated.
- If you do not have a map open, this row reflects the packaging of the configuration you were using in your previous map session.
- If you have never had a map open, this row does not appear.
- If the device has been added to the network since the last time you saved your configuration, this row does not appear.

Administrator user also see a read and a write community string for a device. These values are taken from the list of community strings; however:

- strings from the list appear here only if they are valid.
- only a single valid string appears here even if the list has multiple valid strings for this device.
- the read string that appears here is the string that Network Discovery is currently using to poll the device.

Ports

Provides information about the IP addresses and/or MAC addresses of a device's ports. The information comes from the Network Explorer.

This table has hyperlinks for all the ports with addresses. If a port does not have an address, it does not appear. To open a Port Manager, click a port hyperlink. Each table row contains either:

- a MAC address, an OUI abbreviation (if known), and a manufacturer (if known)
- an IP address, a netmask (if known), and a domain name (if known)

A special port of "Device" is used:

- for the IP or MAC address that Network Discovery identifies as the primary IP or MAC address for the device
- when Network Discovery does not know which port an IP or MAC address is associated with

Table 4: Ports table

Data	Notes
Port index	port number and description
MAC address	—
OUI	—
Manufacturer	usually hyperlinked to an external web site
IP address	—
Netmask	in octet notation
Domain name	—

The ports table is particularly useful:

- When the device is
  - a router
  - a device with multiple IP addresses and domain name aliases (such as a web server)
- When you want to know a device's domain name (and domain name is not included in the list of **Device Title Preferences**)

Exceptions

If there are any exceptions for the device, they are noted in this table. For a complete list of exceptions in your network, see **Reports** >**Support** > **Summary of network exceptions** (*Support Reports* on page 276).

Table 5: Exceptions table

Data	Notes
Severity	alarm | warning | info
Exception	■ exception ■ details (optional)
Explanation	■ description ■ effect ■ action

State

Displays current values for attributes. Displays alarms and warning signals even when the device priority is less than the minimum priority for a configuration (unlike in map windows).

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

Details

Heading

The heading also appears in the Configuration, Ports State, Ports Statistics, and Diagnosis panels (when available).

Table 6: Heading elements

Element	Notes	Type
Icon	for a complete list, see Figure 11-5 and Figure 11-6 on page 205	all
Device type	for a complete list, see **Help** > **Device Types**	all
Device tag	see *Tag* on page 116	real
Virtual device map title	see *Virtual devices* on page 121	virtual
No. of port indexes	"port index" is used instead of "port" because the numbers for the index and the physical port may not match	all
No. of connections	includes user-assigned connections	all
Icon flag	appears if assigned by an Administrator or IT Manager account	
Object title	first title available; see *Title* on page 208	all
Address	IP address; will not appear if identical to object title	real
Title flag	appears if assigned by Prime configuration or user	all
Priority	see *Priority* on page 28	all
Priority flag	appears if assigned by user	all
Virtual device number	created by Network Discovery or by an Administrator or IT Manager account	virtual

Attributes

See **Help** > **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.

Note: The Peregrine appliance itself will have the most attributes because you will see attributes for the appliance, and for the network as a whole.

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. Network 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. To change the time before data is considered stale, see *Account Properties* on page 282.

The left-most column is for attributes that are associated with fault category buttons on the Health Panel—Breaks, Packet Loss, Changes, NEWS, MTTR, or MTBF. The signal light in this column tells you at a glance if the device is experiencing problems.

A neutral signal light indicates that data is not available for a device or port.

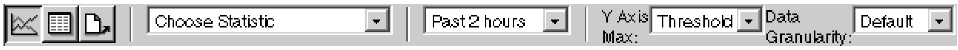
Unlike in map windows, displays alarms and warning signals even when the priority for the port's device is less than the minimum priority for a configuration.

Statistics

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 182).

Figure 11-2: Statistics toolbar



Choose Statistic | Past 2 hours | Y Axis Max: Threshold | Data Granularity: Default

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.

Options

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. The exception to this rule occurs at the beginning of data collection; then Network Discovery shows whatever data it has at five-minute intervals—even if you want to see statistics for long periods of time.

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 and warning thresholds (in the default alarm and warning colors).

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 Network Discovery.

Statistics

Available statistics depend on the device model.

Notes on some statistics:

- *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. Network 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.

Periods

Daily views have statistics averaged every 5 minutes. Monthly views have data averaged every hour. Yearly views have data averaged every day. However, if Network Discovery has been running less than 30 days, yearly views have data averaged every hour (by default).

Limits

period: 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: Threshold Max | Data Max | AttributeMax

Note: 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.

Ports

Lists ports for this device and summarizes the information available for them. Displays 24 ports at a time, with Previous and Next buttons and an All button that shows all ports in a single panel.

The Configuration panel and Ports panel are the most commonly used ways of starting the Port Manager. The Port Manager cannot be launched from the Network Map.

Heading

The heading also appears in the Configuration, State, Ports Statistics, and Diagnosis panels (when available).

Table 7: Heading

Element	Notes	Type
Icon	for a complete list, see Figure 11-5 and Figure 11-6 on page 205	all
Device type	for a complete list, see **Help** > **Device Types**	all
Device tag	see *Tag* on page 116	real
Virtual device map title	see *Virtual devices* on page 121	virtual
No. of ports	the number Network Discovery uses for the port may not match the physical port	all
No. of connections	includes user-assigned connections	all
Icon flag	appears if assigned by an Administrator or IT Manager account	
Object title	first title available; see *Title* on page 208	all
Address	IP address; will not appear if identical to object title	real
Title flag	appears if assigned by Prime configuration or user	all
Priority	see *Priority* on page 28	all
Priority flag	appears if assigned user	all
Virtual device number	created by Network Discovery or by an Administrator or IT Manager account	virtual

Status

Provides information about the IP addresses and/or MAC addresses of a device's ports.

Table 8: Status table

Data	Notes
Port Index	■ hyperlink to the Port Manager ■ "v." indicates a virtual port
Link Status	■ alarm | OK | neutral (will never be warning) ■ also appears in the Port Manager's Configuration panel

Table 8: Status table (Continued)

Data	Notes
Details	■ interface type ■ interface speed ■ duplex
Utilization	■ percentage ■ a single value for half duplex connections ■ two values (in and out) for full duplex connections
Errors	■ per second ■ combined value for in and out ■ only reports errors that a device stores in its MIB ■ Network Discovery does not control and cannot report which errors are included ■ Network Discovery may combine multiple MIB variables into a single error counter
Connected to	hyperlinks to the Device Manager, Port Manager, and Line Manager

Details

Each row in the Ports Statistics table has four main elements:

- the port index
- the port properties
- the port status
- the connection

Only the port index is mandatory, and it always appears with at least one of the other three parts, never by itself.

A neutral signal light indicates that data is not available for a device or port.

Table 9: Details table

Data	Notes
Port Index	hyperlink to the Port Manager
properties (not labelled)	from the MIB, includes: ■ interface type ■ interface speed ■ duplex ■ alarm type (from the Network Discovery Rulebase)
Link Status	alarm | OK | neutral (will never be warning) ■ also appears in the Port Manager’s Configuration panel
Breaks	alarm | warning | OK | neutral
Utilization Status	alarm | warning | OK | neutral
Utilization In*	percentage
Utilization Out*	percentage
Frames In	per second

Table 9: Details table (Continued)

Data	Notes
Frames Out	per second
Bytes In	per second
Bytes Out	per second
Unicasts In	per second
Unicasts Out	per second
Broadcasts Status	alarm | warning | OK | neutral
Broadcasts In	per second
Broadcasts Out	per second
Collisions Status	alarm | warning | OK | neutral
Collisions	■ per second ■ only available on devices that report collisions in the MIB (usually in the dot3StatsEntry object)
Errors Status	alarm | warning | OK | neutral
Errors In	■ per second ■ only reports errors that a device stores in its MIB ■ Network Discovery does not control and cannot report which errors are included ■ Network Discovery may combine multiple MIB variables into a single error counter
Errors Out	
Delays Status	alarm | warning | OK | neutral
Delays Value	in milliseconds
MTTR Status	alarm | warning | OK | neutral
MTTR Value	hours
MTBF Status	alarm | warning | OK | neutral
MTBF Value	days
connected to (not labelled)	hyperlinks to the Device Manager, Port Manager, and Line Manager

* For half duplex connections, a single value is shown: Line utilization.

Port Index

The term "port index" is used instead of "port" because the numbers for the index and the physical port may not match.

Properties

The port properties come from the MIB. Each property can be changed in the Port Manager. The properties consist of:

- interface type description
- interface speed
- duplex
- alarm type description

Status

Displays the status and statistics for every port.

Parentheses around statistics means that no data is available for the current poll cycle. Data shown are from a recent previous poll cycle.

Note: Usually stale data is gray, but in this panel parentheses indicate stale data.

Connection

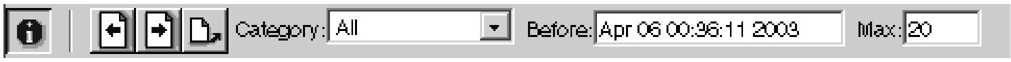
Displays what each port on the current device is connected to. Shows both the target device and the port of the target device. The target device and target port are both hyperlinked.

Events

Provides an additional toolbar to help you view events that occurred to the device or the device's ports over a specified period. What events are logged depends on how event filters have been set up.

Related For detailed information, see *Chapter 16, Events Browser*.

Figure 11-3: Events toolbar



Category: All

Before: Apr 06 00:36:11 2003

Max: 20

Event entry

Each row in the Events panel contains the following columns.

Table 10: Events data

Data	Limits/Options	Notes
Date/Time	—	—
State	alarm | warning | OK | neutral | info	signal light
Category	Line Breaks | Utilization | Delay | Collisions | Broadcasts | Errors | Device Breaks | Packet Loss | Adds | Deletes	—
Priority	1–6	must be greater or equal to the priority in "log-events-line" and "log-events-device" (default is 3)
Device type	see *Device identification* on page 26	small device icon and tag
Device (Port)	—	device title, followed by port in parenthesis—if the traffic can be identified as inbound or outbound, this will also be noted—both are hyperlinked
Value		■ Broadcasts | Errors: frames per second ■ Utilization | Packet Loss: percentage ■ Delay: response time in milliseconds ■ Collisions: collisions per second ■ Line Breaks | Device Breaks | Adds | Deletes: no value shown

Note: The priority for each entry is based on the Prime configuration.

Broadcast warnings are not logged, due to the potentially very high number of events. Broadcast alarms are logged.

Toolbar

Events

Updates the window with the most recent events.

Older

Updates the window with earlier events, relative to currently displayed events.

Newer

Updates the window with later events, relative to currently displayed events. An alternative to entering a specific time and date in the Before field, which updates the window absolutely.

Export

Exports selected events to a Comma Separated Value (CSV) file or XML file.

Table 11: Events parameters

Parameter	Limits	Default
From	January 1, 1970–December 31, 2037	—
To	January 1, 1970–December 31, 2037	—
Category	All | Line Breaks | Utilization | Collisions | Broadcasts | Errors | Device Breaks | Packet Loss | Changes	current selection
Max	1–1000	1000

Category

Selects the category of events for display so that you can focus on a specific event type.

Before

Set the time and date for the first entry in the window absolutely. An alternative to the **Older** and **Newer** buttons, which change the display relatively.

Max.

Set the maximum number of events per window.

Diagnosis

Displays information about the current state of the device that can be helpful in diagnosing problems. Has buttons that give you access to diagnostic tools. Opens with a configuration panel.

(Diagnosis) configuration

Heading

The heading also appears in the Configuration, State, Ports State, and Ports Statistics panels (when available).

Table 12: Heading

Element	Notes	Type
Icon	for a complete list, see Figure 11-5 and Figure 11-6 on page 205	all
Device type	for a complete list, see **Help** > **Device Types**	all
Device tag	see *Tag* on page 116	real
Virtual device map title	see *Virtual devices* on page 121	virtual
No. of ports	the number Network Discovery uses for the port may not match the physical port	all
No. of connections	includes user-assigned connections	all
Icon flag	appears if assigned by an Administrator or IT Manager account	
Object title	first title available; see *Title* on page 208	all
Address	IP address; does not appear if identical to object title	real
Title flag	appears if assigned by Prime configuration or user	all
Priority	see *Priority* on page 28	all
Priority flag	appears if assigned user	all
Virtual device number	created by Network Discovery or by an Administrator or IT Manager account	virtual

Beneath the heading, this panel is divided into four main sections:

- Main Diagnosis
- Network Configuration
- Device Management
- Properties Inheritance

Main Diagnosis

The main table indicates the data flow for this device—when the device was first and most recently seen by various parts of Network Discovery—plus the current values for several parameters.

Table 13: Main Diagnosis table

Data	Output	Notes
First discovered	elapsed time* / absolute date & time	Reset if database is cleared.
Added to map	elapsed time / absolute date & time	Resets if the device is trashed, but then returns to the map.
Last seen	elapsed time / absolute date & time	in ping or poll by Network Discovery
Last changed	elapsed time / absolute date & time	the last time a connection to this device changed
Network model last updated	elapsed time / absolute date & time	the last time the model changed; determines whether or not the model has been for this device
Device checked for existence	elapsed time / absolute date & time	the last time a device was pinged for discovery; should be “n/a” or a time before “Model last updated”
Last trashed	elapsed time / absolute date & time	the last time a device was put into the trash
Mean break diagnosis time	minutes for alarms; minutes for warnings	Mean break diagnosis time is approximate. Diagnosing a break fault may take longer, if communication with the device is unreliable.
Device modeler interval	either “Default as set in Network Configuration.” or time (in days, hours, minutes, seconds)	If custom, is shown here.
Mean device modeler update run time	elapsed time	the mean length of time it takes to update the model for this device the previous 4 times
Recent device modeler update run times	elapsed time	the length of time it took to update the model for this device the previous 4 times
Rulebase ID	—	an internal number

* Elapsed time is reported in at least two of the following units: weeks, days, hours, minutes, and seconds. As elapsed time increases, the finer units of measure are not reported.

Network Configuration

The Network Configuration table shows what parameters have been set up for the range in which the device resides and what their values are. (It shows the Network Properties, (**Administration** > **Network Configuration**)

Options

Network Properties include:

- Allow devices

- Actively ping
- Net BIOS query
- Resource manage
- Force ARP table read
- Accumulate IP addresses
- Allow IP addresses
- Allow ICMP and SNMP
- Service manage
- Device Modeler interval

Network Properties may be set to On, Off or Inherit

Community read strings and write strings include names of Community Property Groups or Sets that have been applied to the range in which the device occurs.

- Bandwidth
- Frequency
- Scanner run schedule
- Scanner upgrade schedule
- Scan file download schedule
- Listener communication ports

Device Management

Device Management indicates whether or not a device supports collecting of several types of data—specifically, whether or not the device has returned at least one valid piece of data in the preceding 2 weeks.

The device management table indicates exceptions that may make it possible to determine whether or not a device is functioning properly. For example, if you are examining a switch and notice that it does not support bridge tables, there is a problem somewhere. Similarly, if you are examining a workstation and see that it does support bridge tables, then there is also probably a problem.

Table 14: Device Management table

Data type	Output	Determining factor	Uses
Polls	Yes | No	■ provides traffic counters ■ has recently returned a valid poll	■ to determine utilization statistics ■ to determine connectivity when no bridge table or ARP table information is available
Source Address Capture	Yes | No	has recently returned a poll line with a non-zero source address	to determine connectivity
Bridge	Yes | No	has recently returned a bridge table entry with a non-zero MAC address	to determine connectivity

Table 14: Device Management table (Continued)

Data type	Output	Determining factor	Uses
ARP	Yes | No	has recently returned a valid ARP entry	■ to determine connectivity ■ to relate MAC and IP addresses
SNMP	Yes | No	has recently had at least one port defined as being managed	■ to obtain information from the MIB ■ to determine break fault status

Properties Inheritance

The properties inheritance table helps you to determine the rules Network Discovery has used to assign the title, icon, and priority to the device.

Certain object properties, such as device titles, cascade from the Prime configuration provided the configuration has not had a property assigned by the user. User-assigned properties always take precedence, even over the cascade. One property that does not cascade under any circumstances is priority.

Table 15: Properties Inheritance table

Parameter	Notes
Default title	—
Default title from	Network Discovery Generated, (*Device Title Preference* on page 369) One of: | Device-specific title| Domain name* | NetBIOS name (network)* | NetBIOS name (scan) | Asset tag | BIOS asset tag | Last name| First name | Operating system | Family | Model | Network function | System description* | System name* | System location* | System contact* (*requires that the device have an IP address)
Prime-assigned title	takes precedence over default
User-assigned title	takes precedence over Prime
Default icon	—
Administrator-assigned icon	icon assignment is always applied with the next poll cycle, and is not associated with any map configuration
Default priority	—
Prime-assigned priority (no cascade)	for information only; never affects active configuration; useful if you receive e-mail or a page from Network Discovery
User-assigned priority	—

If no value has been assigned, an asterisk (*) appears in this table, indicating that the value for the property comes from the previous row of the able.

IP Ping

Pings the device to see if it responds, and how quickly. The IP address pinged is the address identified by Network Discovery as the primary IP—see *State* on page 182.

Limits

- 1–20 pings
- The device must have an IP address. If not, this button is dimmed.

Default

5 pings

Traceroute

Displays the path that data takes to get from the Peregrine appliance to the selected device by listing the gateway devices associated with each hop of the journey. The device identifier is often the host name, where available, but can also be the IP address. Each device title is hyperlinked to a Device Manager.

Traceroute also displays the amount of time each hop took. This time is the round trip in milliseconds. Traceroute includes two retry hops for each try, so the times for all three hops are shown.

Traceroute helps you to understand where on the network problems are occurring. It is often used after *IP Ping* on page 196 has been used to confirm the existence of a device.

Note: The path displayed by traceroute is at OSI layer 3 and may not match the connectivity on the Network Map or in the *Service Analyzer* on page 198, which map at layer 2.

When to use it

- If you suspect that you are losing packets due to a large hop count.

  In a TCP/IP network, where data are transmitted in packets, the header for a packet tracks the hop count. If the hop count grows too large, the packet is discarded.
- If you are trying to determine the point along the path where traffic is slowing down or getting lost altogether.
- If you are trying to determine the precise path taken—not so much to solve a problem as for general information.

Limits

The device must have an IP address. If not, this button is dimmed.

Output

Results of an asterisk for the device and for all three times (i.e. the result * * * *) indicates that data is not available for that hop of the journey, and usually indicates a trouble spot along the path. The following table explains codes you may see when you attempt a Traceroute.

Table 16: Traceroute special results

Chars.	Meaning
*	no response within a 3-second timeout interval
!	ttl <= 1*

Table 16: Traceroute special results(Continued)

Chars.	Meaning
!H	host is unreachable
!N	network is unreachable
!P	protocol is unreachable
!S	source route failed
!F	fragmentation needed
!X	communication is prohibited administratively
!V	a host precedence violation has occurred
!C	precedence cutoff is in effect

* The ttl value is supposed to start at 1 and increase by 1 until the host is reached.

Related

To see the OSI layer 2 path between any two devices, see also *Service Analyzer* on page 198.

SNMP Ping

Queries the device for basic SNMP information and displays this information. The IP address pinged is the address identified by Network Discovery as the primary IP—see *State* on page 182.

Limits

The device must have an IP address. If not, this button is dimmed.

Default

- Demo, IT Employee, IT Manager: “public”
- Administrator: the read community string for the device as defined in **Administration** > **Network configuration** > **Community Property Groups**.

DNS Query

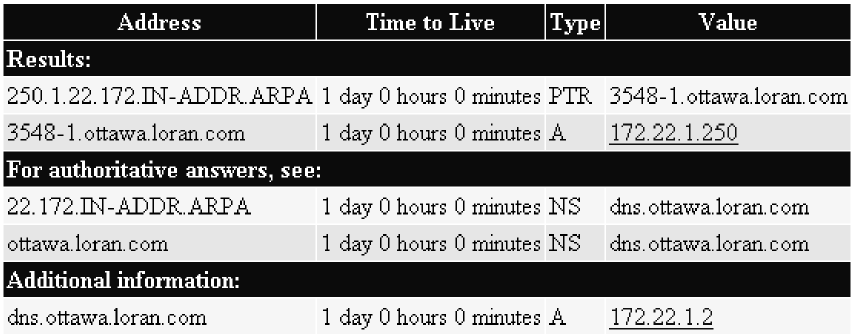
Sends a host query to the domain name server and displays a table that highlights configuration errors. A highlighted line indicates that the next line in the progression is missing.

The highlighted configuration errors are:

- a pointer (PTR) without an IP address (A or AAAA)
- duplicate pointer (PTR) records for the same IP address (A or AAAA)
- a mail exchanger (MX) directed to a canonical name (CNAME)
- a canonical name (CNAME) directed to anything that doesn't exist

If no information in the table is highlighted, Network Discovery did not detect any problems with the DNS configuration of the device.

Figure 11-4: Example of a DNS Query table



Address	Time to Live	Type	Value
Results:			
250.1.22.172.IN-ADDR.ARPA	1 day 0 hours 0 minutes	PTR	3548-1.ottawa.loran.com
3548-1.ottawa.loran.com	1 day 0 hours 0 minutes	A	172.22.1.250
For authoritative answers, see:			
22.172.IN-ADDR.ARPA	1 day 0 hours 0 minutes	NS	dns.ottawa.loran.com
ottawa.loran.com	1 day 0 hours 0 minutes	NS	dns.ottawa.loran.com
Additional information:			
dns.ottawa.loran.com	1 day 0 hours 0 minutes	A	172.22.1.2

Limits

If the device does not have an IP address, the button is dimmed.

Procedural alerts

If Network Discovery displays the message "Non-existent domain", it means that the device has not been assigned a domain name.

Locate

Highlights within a map window the location of the device.

▶ Click **Locate**.

A map window opens. Within the window, the device has a purple rectangle around it.

If the window containing the device was already open, that window becomes the front-most window, and the window scrolls so that you can see the highlighted icon.

Service Analyzer

Opens the Service Analyzer query window with the current device already selected as Device 1, to allow the user to view the state of the path between this device and any other device on the Network Map. See also *Chapter 15, Service Analyzer*.

Manage

Launches an element manager of your choice.

Limits

- The device must be a real device. If not, this button is dimmed.
- The URL or application must defined in *The screen shows the current settings. The default is to package all classes, and to create the generic End Node class last.* on page 373. If not, this button is dimmed.

Note: *for Aggregator*—This button is never dimmed when you are viewing a remote appliance from the Aggregator appliance.

Procedural alerts

Note: *for Netscape 4.x*—The first time you manage by means of an application specific to a platform, you will be asked to grant permission.

Note: *for Aggregator*—Definitions for *The screen shows the current settings. The default is to package all classes, and to create the generic End Node class last.* on page 373, are supplied from the Aggregator appliance, not the remote appliance.

Related

To specify a URL or application for this button, see *The screen shows the current settings. The default is to package all classes, and to create the generic End Node class last.* on page 373.

Browse MIB

Opens the MIB Browser to allow the user to view the device's SNMP MIB. See also *Chapter 17, MIB Browser*.

The MIB Browser also allows an expert user with an Administrator or IT Manager account to manipulate the device on a more detailed level.

Limits

- The device must have an IP address. If not, this button is dimmed.
- The device must support basic SNMP functionality.

View Scan Data

Opens an Asset Viewer window to show information about the device collected by the Peregrine's Express Inventory, the Windows Management Instrumentation (WMI) Collector. For information on setting up and using the WMI Collector, see your ServiceCenter Essentials documentation.

Also opens an Asset Viewer window to show information about the Peregrine appliance collected by Peregrine's Desktop Inventory scanner. For more information, see your Peregrine Desktop Inventory documentation.

Limits

If you do not have Peregrine's Express Inventory, the WMI Collector installed, an Asset Viewer window does not open for the device.

If there is no scan data, the View Scan data button is dimmed.

Web

Attempts to open a web browser window for the device.

When to use it

If the device supports web-based management or other web services.

Limits

- The device must have an IP address. If not, this button is dimmed.
- The device must support HTTP sessions. (Network Discovery does not check before attempting a connection.)

Related

To control how HTTP connections are made, see *Appliance Proxy Services* on page 358.

Note: for Aggregator—See also *Remote Appliance Properties* on page 327.

Telnet

Attempts to open a Telnet session. Many network devices provide Telnet as a means to set up and configure the device.

Limits

- The device must have an IP address. If not, this button is dimmed.
- The device must support Telnet sessions. (Network Discovery does not check before attempting a connection.)

Related

To control how Telnet connections are made, see *Appliance Proxy Services* on page 358.

Note: for Aggregator—See also *Remote Appliance Properties* on page 327.

Update Model *[Administrator or IT Manager only*]

Puts this device at the top of the device modeler's queue.

Tries all valid community strings for this device, in the order specified in **Administration** > **Network Configuration** > **Community Property Groups**. Does not begin with the currently active community string. Begins with the first string in the list of community strings.

Note: There may be a delay of as much as 1–2 hours before the device appears on the Network Map.

Network Discovery checks several conditions before updating a device model.

Table 17: Conditions for updating device model

State	Message
alarm	IP address is not in scope
alarm	no read community strings have been specified
warning	no write community strings have been specified
warning	IP address is not in scope for resource management
info	current discovery process
info	list of read community strings to be tried
info	list of write community strings to be tried
info	update interval
info	mean time to update model

When to use it

- When you've made changes to a device that affect connectivity—for example, when you've changed cards in a router.
- When you've made changes to a device's community strings.

Limits

The device must have an IP address. If not, this button is dimmed.

Related

To determine when a model was last updated, see *Diagnosis* on page 192, under "Network model last updated".

Purge device *[Administrator or IT Manager only*]

Removes a device from the Network Map.

Warning: This action cannot be undone.

Warning: Purging a device always affects the configurations of all accounts, even if **Save As Prime** [Administrator or IT Manager] is not used.

Important: You are *not* making a physical change to the device or network. If you purge a device but the device is still present in your network and still operational, Network Discovery will rediscover the device and the device will reappear on the Network Map. To prevent the device from reappearing, you must actually disconnect the device from your network, or you must apply to the device a Network Property Group or Set with the property, “Allow devices” set to “Off” (**Administration** > **Network Configuration** > **Network Property Groups**—see *Network Configuration* on page 317).

If a device has not been seen for the period set (in **Administration** > **Network Tuning** > **Expiry** > **Device Purge Intervals**—see *Expiry* on page 352), Network Discovery automatically purges it.

When to use it

When a device has been removed from the network and you wish to update the Network Map.

Effects

- Deletes the statistical history associated with the device. This in turn affects the graphs and reports for this device.
- Deletes the events associated with the device from the event log.

Limits

- Available to any combination of single and multiple devices and packages.
- Not available when using the **Forecast** command to view the Network Map.
- *Time to take effect:* start of the next poll cycle

Related

- To adjust how long Network Discovery waits before automatically purging a device, see Device Purge Intervals in *Expiry* on page 352.
- You can also purge a device by using the Network Map menu—see *Purge [Administrator or IT Manager only]* on page 162 in chapter *10*, *Network Map Menus*.
- Right-click: You can also find **Purge** [Administrator or IT Manager only] on right-click menus for packages and multiple objects.
- To purge a port, see *Purge Port [Administrator or IT Manager only]* on page 226.
- To purge an attribute, see *Purge Attribute [Administrator or IT Manager only]* on page 246.

Properties

Modifies properties of an object. Properties affect an object’s appearance, priority, and placement within a map window.

Tip: To have changes to a device’s properties reflected when you open a Device Manager for the object, you must save your map configuration. See *Save* or *Save As…* on page 132.

Administrator or IT Manager: Device icons can only be changed by an Administrator or IT Manager user.

Effects

Changing a device icon:

- affects device type
- can affect priority
- can affect events notification and logging
- can affect packaging

Warning: Changing a device icon always affects the configurations of all accounts and event filters, even if **Save As Prime** [Administrator or IT Manager only] is not used. Changes take effect almost *immediately* (at the beginning of the next poll cycle).

Options

Whether or not an object property can be change depends on the type of object you have selected and the type of account you are using.

Table 18: Ability to change properties

Option	Object type	Account type
Icon	device (real or virtual)	Administrator or IT Manager only
	package	all
Title	device (real or virtual), package	Administrator or IT Manager: Prime map configuration affects other accounts
Priority	device (real or virtual)	all
Top of Network	device (real or virtual), package	all

Limits

- Must be used on one object at a time. Not available to an empty package.
- *Icons:* see Figure 11-5 and Figure 11-6 on page 205
- *Titles:* input: 1–80 characters; display: 1–20 characters; valid characters: A–Z, a–z, 0–9, *(space), (most punctuation, excluding* ' [*single quote*], *and* " [*double quote*] *)*
- *Priority:* 1–6; see *Priority* on page 28

Note: If the Network Map is not already open when you click **Properties**, Network Discovery asks you to confirm that it is OK to open one now.

Figure 11-5: Device icons

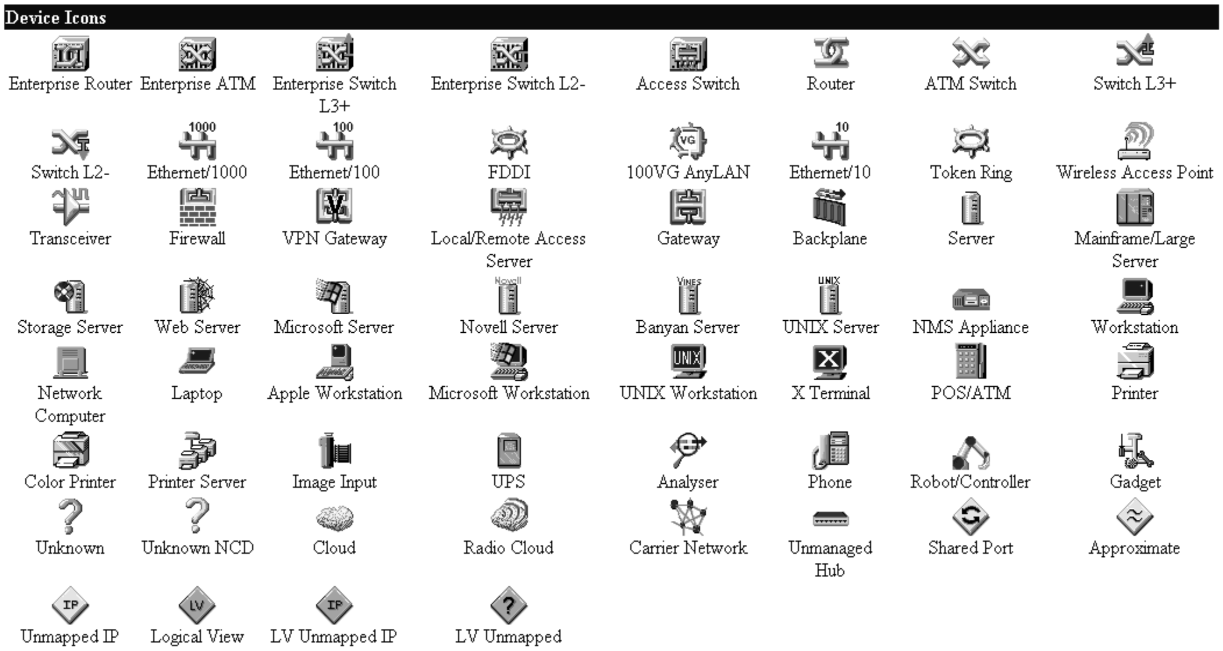
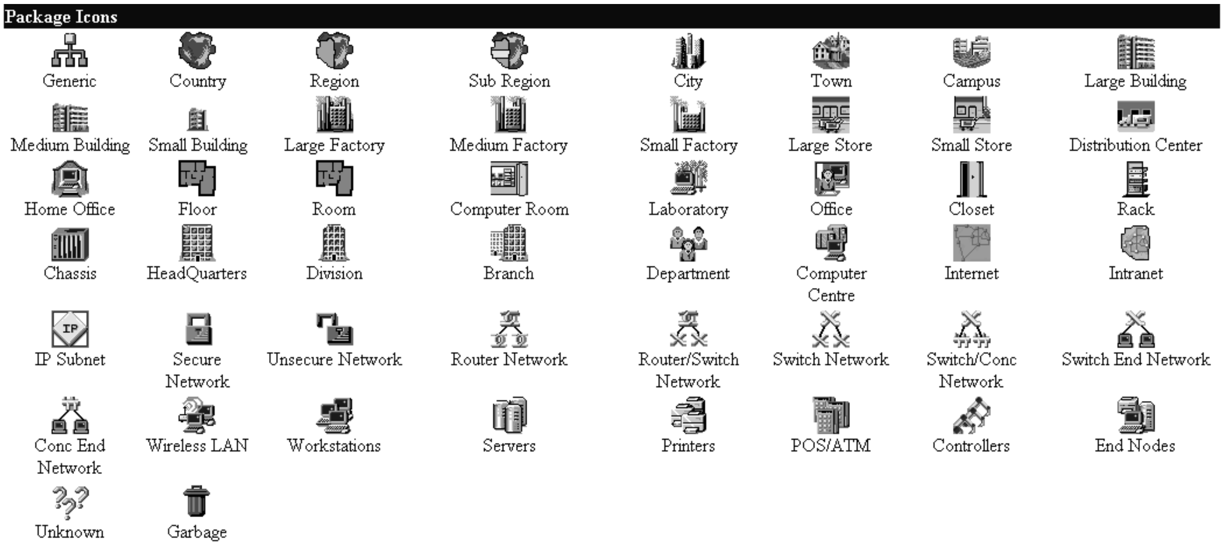


Figure 11-6: Package icons



Refresh

Refreshes the contents of the panel.

When used with IP Ping and SNMP Ping panels, uses the last entered value instead of prompting you for a value.

Limits

Does not re-read the data in the panel from the network. Re-reads the data only from the Network Discovery database.

Does not affect Properties or Locate panels, or any of the interactive session windows (Browse MIB, Web, Telnet).

Print

Sends the contents of the panel to a printer attached to the management workstation.

Text

Displays the contents of the Device Manager as text that can be copied and pasted.

Note: If the Statistics Graph panel is displayed, the Text button displays a text version of the Table, since there can be no text version of a graph.

Note: May cause the panel to be refreshed with new data.

Procedural alert

To return to non-text mode, click the currently depressed button again.

Close

Closes the window and exits the Device Manager.

Panel Elements

Note: If information displayed in the Device Manager does not match the information as displayed on the Network Map, trying saving your map configuration. See *Save* or *Save As…* on page 132.

Common Elements

Certain elements are common to all Device Manager panels:

- 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. (In some cases, data may be shown in parentheses rather than with a gray background.) To change the time before data is considered stale, see *Account Properties* on page 282.
- A neutral signal light indicates that data is not available for a device or port.
- The final line on each panel is the date and time that the panel was refreshed. (This refers to rendering the panel itself, not when the data shown in the panel was last read.) This date can be useful for when you print a panel. To change the format of this date, see *Account Properties* on page 282.

Banner

The banner that appears at the top of all Device Manager panels consists of four elements.

Table 19: Device Manager banner

Element	Example	Notes
Device title and IP address	website.example.com / 192.168.96.1	■ see *Title* on page 208 ■ if the device title is the IP address, the IP address is shown once ■ if there is no IP address, only the device title is shown
Manager name	Device Manager	—
System name of Peregrine appliance	ExampleCorp	see *Appliance System Variables* on page 294
Web browser name	Netscape | Internet Explorer	—

Title

Options

The title displayed in the banner of the Device Manager window and in the heading of Configuration and State panels will be the first available of:

- user-assigned name
- Prime-assigned name
- *virtual devices only:* Network Discovery generated name
- a device title chosen by the Network Discovery Administrator in **Administration** > **Display Preferences** > **Device Title Preference**; (see *Device Title Preference* on page 369). The Network Discovery Administrator can choose one or several of the following and choose their order too:
    - Asset Tag
    - BIOS Asset Tag
    - NetBIOS Name (scan)
    - Last Name
    - First name
    - Device-specific title
    - Domain name
    - NetBIOS name (network)
    - Operating system
    - Family
    - Model
    - Network function
    - System description
    - System name
    - System location
    - System contact
- IPv6 address
- IPv4 address
- MAC address including OUI
- MAC address (all-numeric)

Titles from the Prime configuration are inherited when you open your configuration. The only way to prevent the Prime title from being used is to assign a title yourself by using *Properties* on page 159. You cannot force the use of the default device title instead. (To determine the default title, see the *Diagnosis* panel.)

12 Port Manager

CHAPTER

- To explore icon buttons in the toolbar menus, see:
  - Manager toolbar (page 210)
  - Statistics toolbar (page 217)
  - Events toolbar (page 219)
- To interpret data in the Port Manager window, see *Panel Elements* on page 231.
- To select a different port for the same device, use the port list box—see *Port number* on page 228.

Introduction

Provides you with detailed information about a device's ports, in one of several panels.

Administrator or IT Manager: Also enables you to change the way Network Discovery perceives a connection.

Note: The Port Manager enables you to change only Network Discovery's perception of a connection. The Port Manager does not change the physical connection.

Important: The Port Manager options that are only for Administrator or IT Manager accounts require you to make changes to all accounts and all map configurations.

Ways of opening

Click a port hyperlink from:

- the Device Manager's State panel
- the Device Manager's Ports panel
- the Line Manager
- the Events Browser
- a report

Default panel

- *initial:* State
- *subsequent:* from *Account Properties* on page 309

Toolbar

Availability of buttons in the Port Manager toolbar.

Table 1: Available toolbar buttons

Icon	Button name	Page	Regular or demo user
i	Configuration	page 211	YES
!	State	page 213	YES
	Diagnosis	page 214	YES
Σ	Statistics	page 217	YES
	Events	page 219	YES
	Locate	page 221	YES
	Interface Rate [Administrator or IT Manager only]	page 221	—
?	Interface Type [Administrator or IT Manager only]	page 222	—
!	Alarm Type [Administrator or IT Manager only]	page 224	—
	Duplex Mode [Administrator or IT Manager only]	page 226	—
X	Purge Port [Administrator or IT Manager only]	page 226	—
	Create Connection [Administrator or IT Manager only]	page 227	—
	Break Connection [Administrator or IT Manager only]	page 227	—

Configuration

Identifies a port and presents an overview of the port's identity and connections.

Details

This panel is divided into three main sections:

- Heading
- Connectivity table
- Identity table

Heading

The heading also appears in the *State* and *Diagnosis* panels (when available).

Table 2: Heading elements

Element	Notes	Type
Device Icon	for a complete list, see Table 11-5 on page 205 and Figure 11-6 on page 205	all
Device type	for a complete list, see **Help** > **Device Types**	all
Device tag	see *Tag* on page 116	real
No. of ports	the number Network Discovery uses for the port may not match the physical port	all
No. of connections	includes user-assigned connections	all
Icon flag	appears if assigned by an Administrator or IT Manager account	all
Object title	first title available; see *Title* on page 208; hyperlinked to Device Manager	all
Port no./ description	number of port / description of port	all
Title flag	appears if assigned by Prime configuration or user	all
Device priority	see *Priority* on page 28	all
Priority flag	appears if assigned user	all

Connectivity

Most information in this table comes from the Network Discovery Rulebase.

Table 3: Elements of Identity table in Configuration panel

Data	Example	Notes
Connected to	the selected port is connected to another device on this port	hyperlinked to Device Manager, Port Manager, and Line Manager
Description	100Base-TX Port	from device manufacturer
Interface type	Ethernet CSMA/CD	from device MIB/Network Discovery Rulebase
Interface flag	(assigned by Administrator or IT Manager)	appears if assigned by an Administrator or IT Manager account

Table 3: Elements of Identity table in Configuration panel (Continued)

Data	Example	Notes
Alarm type	Ethernet 100 HD	from device MIB/Network Discovery Rulebase
Alarm flag	(assigned by Administrator or IT Manager)	appears if assigned by an Administrator or IT Manager account
Interface rate	100 Mbits/sec.	from device MIB/Network Discovery Rulebase
Rate flag	(assigned by Administrator or IT Manager)	appears if assigned by an Administrator or IT Manager account
Duplex	Half	Half | Full
Duplex flag	(assigned by Administrator or IT Manager)	appears if assigned by an Administrator or IT Manager account

Identity

This table identifies the port and the manufacturer of the device:

- MAC address of the port
- OUI of the device (alphabetic abbreviation of the device manufacturer)
- Manufacturer of the device, hyperlinked to manufacturer’s web site

State

Heading

The heading also appears in the *State* and *Diagnosis* panels (when available).

Table 4: Heading elements

Element	Notes	Type
Device Icon	for a complete list, see Figure 11-5 and Figure 11-6 on page 205	all
Device type	for a complete list, see **Help** > **Device Types**	all
Device tag	see *Tag* on page 116	real
No. of ports	the number Network Discovery uses for the port may not match the physical port	all
No. of connections	includes user-assigned connections	all
Icon flag	appears if assigned by an Administrator or IT Manager account	all
Object title	first title available; see *Title* on page 208; hyperlinked to Device Manager	all
Port no./ description	number of port / description of port	all
Title flag	appears if assigned by Prime configuration or user	all
Device priority	see *Priority* on page 28	all
Priority flag	appears if assigned user	all

Table

There is a list of supported device and port attributes in Network Discovery Help.

These values are collected from the network regularly (at the end of each poll cycle) 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 *Account Properties* on page 282.

The left-most column is for attributes that are associated with fault category buttons on the Health Panel—Breaks, Utilization (In, Out and Line), Delay, Broadcasts (In and Out), Collisions, Errors (In and Out). The signal light in this column tells you at a glance if the port is experiencing problems.The column also includes Operational Status. The indicator light for Operational status shows alarm color = down, OK color = up and neutral color = unknown. The Operational Status light is never the warning color.

A neutral signal light indicates that data is not available for a device or port.

Unlike in map windows, displays alarms and warning signals even when the priority for the port's device is less than the minimum priority for a configuration.

Diagnosis

Displays information about the current state of the port that can be helpful in diagnosing problems with Network Discovery.

This panel is divided into three main sections:

- Heading
- Main table
- Port management

Heading

The heading also appears in the *State* and *Diagnosis* panels (when available).

Table 5: Heading elements

Element	Notes	Type
Device Icon	for a complete list, see Figure 11-5 and Figure 11-6 on page 205	all
Device type	for a complete list, see **Help** > **Device Types**	all
Device tag	see *Tag* on page 116	real
No. of ports	the number Network Discovery uses for the port may not match the physical port	all
No. of connections	includes user-assigned connections	all
Icon flag	appears if assigned by an Administrator or IT Manager account	all
Object title	first title available; see *Title* on page 208; hyperlinked to Device Manager	all
Port no./ description	number of port / description of port	all
Title flag	appears if assigned by Prime configuration or user	all
Device priority	see *Priority* on page 28	all
Priority flag	appears if assigned user	all

Main table

The main table indicates the data flow for this port—when the device was first and most recently seen by various parts of Network Discovery—plus the current values for several parameters.

Table 6: Main Diagnosis table

Data	Output	Notes
First discovered	elapsed time* / absolute date & time	resets if database is cleared
Added to map	elapsed time / absolute date & time	resets if the device is trashed, but returns to the map
Last changed	elapsed time / absolute date & time	the last time a connection to this device changed
Network model last updated	elapsed time / absolute date & time	the last time the model changed; determines whether or not the model has been for this device
Last trashed	elapsed time / absolute date & time	the last time a device was trashed
Mean break diagnosis time	time for alarms; time for warnings	—
Default duplex derived from	Device | Rulebase	—
Connection method	■ bridge tables ■ source address capture ■ traffic ■ link training ■ logical subnet ■ approximate; see *Virtual devices* on page 121 ■ user-defined; see *Create Connection [Administrator or IT Manager only]* ■ unknown	—
Previously connected to	■ none ■ device (real or virtual), hyperlinked to Device Manager ■ device and port, hyperlinked to the Device Manager and Port Manager	if blank, the device is no longer in the database, or the connection has never changed

* As elapsed time increases, the finer units of measure are not reported.

Port Management indicates whether or not a port supports collecting of several types data—specifically, whether or not the port has returned at least one valid piece of data in the preceding 2 weeks.

Table 7: Port Management

Data type	Output	Determining factor	Uses
Polls	Yes | No	■ provides traffic counters ■ has recently returned a valid poll	■ to determine utilization statistics ■ to determine connectivity when no bridge table or ARP table information is available
Source Address Capture	Yes | No	has recently returned a poll line with a non-zero source address	to determine connectivity
Bridge	Yes | No	has recently returned a bridge table entry with a non-zero MAC address	to determine connectivity
ARP	Yes | No	has recently returned a valid ARP entry	■ to determine connectivity ■ to relate MAC and IP addresses
SNMP	Yes | No	has recently had at least one port defined as being managed	■ to obtain information from the MIB ■ to determine break fault status

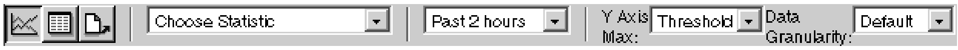
Statistics

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 (*Attributes* on page 182)

Figure 12-1: Statistics toolbar



Choose Statistic

Past 2 hours

Y Axis Max: Threshold

Data Granularity: Default

Options

Graph

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.

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

Gray portions of the graph indicate that data was not available for a period. Lighter gray is used for unavailable average data, darker gray for unavailable peak data. Also shown on the graph are horizontal lines representing alarm and warning thresholds.

Table

The table shows a tabular view of the statistics. Average in and average out are the sum of all the values for each port of the device. For example, if a concentrator has 10 ports, the average output is 10 times the output on each port.

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 Network Discovery.

Statistics

Available statistics depend on the device model.

Notes on certain statistics:

- *Breaks:* This statistic reports cumulative values.
- *Downtime:* This statistic reports cumulative values.
- *Bytes (In/Out):* Some devices do not report traffic in bytes, so this menu item may not appear. For such devices, try Frames (In/Out).

- *Errors (In/Out):* Includes only errors in that the device stores in its MIB. Network Discovery does not control which errors are stored, and cannot report errors that the device does not store.
- *Collisions:* Only available for Ethernet half duplex. Also restricted to devices that report collisions in the dot3StatsEntry object of their MIB.
- *CIR Headroom, CIR Shortfall, Data Delivery Ratio, Frame Delivery Ratio, Discard Eligibility, BECN, FECN:* These statistics are available only for frame relay.

Periods

Daily views have statistics averaged every 5 minutes. Monthly views have data averaged every hour. Yearly views have data averaged every day.

Limits

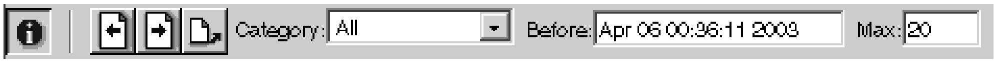
- *period:* Past 2 hours | Past 4 hours | Past 6 hours | Past 12 hours | Past 24 hours | Past 48 hours | Past 7 days | Past 30 days | Past 90 days | Past 180 days | Past 365 days | Today | This week | This month | This quarter | This half | This year | Last week | Last month | Last quarter | Last half | Last year
- *maximum:* Threshold Max | Data Max | Attribute Max

Events

Provides a second toolbar to list all events that occurred to this port over a specified period.What events are logged depends on how event filters have been set up.

Related For detailed information, see *Chapter 16, Events Browser*.

Figure 12-2: Events toolbar



Category: All

Before: Apr 06 00:36:11 2003

Max: 20

Event entry

Each row in the Events panel contains the following columns.

Table 8: Events data

Data	Limits/Options	Notes
Date/Time	—	—
State	alarm | warning | OK | neutral | info	signal light
Category	Line Breaks | Utilization | Delay | Collisions | Broadcasts | Errors | Device Breaks | Packet Loss | Adds | Deletes	—
Priority	1–6	must be greater or equal to the priority in “log-events-line” and “log-events-device” (default is 3)
Device type	see *Device identification* on page 26	small device icon and tag
Device (Port)	—	device title, followed by port in parenthesis—if the traffic can be identified as inbound or outbound, this will also be noted—both are hyperlinked
Value	—	■ Broadcasts | Errors: frames per second ■ Utilization | Packet Loss: percentage ■ Delay: response time in milliseconds ■ Collisions: collisions per second ■ Line Breaks | Device Breaks | Adds | Deletes: no value shown

Note: The priority for each entry is based on the Prime configuration.

Broadcast warnings are not logged, due to the potentially very high number of events. Broadcast alarms are logged.

Toolbar

Events

Updates the window with the most recent events.

Older

Updates the window with earlier events, relative to currently displayed events. An alternative to the Before field, which updates the window absolutely.

Newer

Updates the window with later events, relative to currently displayed events. An alternative to the Before field, which updates the window absolutely.

Export

Exports selected events to a Comma Separated Value (CSV) file or XML file.

Table 9: Events parameters

Parameter	Limits	Default
From	January 1, 1970–December 31, 2037	—
To	January 1, 1970–December 31, 2037	—
Category	All | Line Breaks | Utilization | Collisions | Broadcasts | Errors | Device Breaks | Packet Loss | Changes	current selection
Content	CSV | XML	CSV
Max	1–1000	1000

Category

Selects the category of events for display so that you can focus on a specific event type.

Before

Set the time and date for the first entry in the window absolutely. An alternative to the **Older** and **Newer** buttons, which change the display relatively.

Content

Determine the format of the content to be exported.

Max.

Set the maximum number of events per window in **Administration** > **Account properties** (*Account Properties* on page 282).

Locate

Highlights within a map window the location of the device to which this port is attached.

▶ Click **Locate**.

A map window opens. Within the window, the device has a purple rectangle around it.

If the window containing the device was already open, that window becomes the front-most window, and the window scrolls so that the highlighted icon can be seen.

Interface Rate *[Administrator or IT Manager only*]

Sets rate for a line interface.

When to use it

- When you want to set a custom line speed
- When Network Discovery has set the wrong line speed.

Limits

0 bit/sec.–2 Gbit/sec.

Effects

- Interface rate affects utilization statistics.
- Changing interface rate affects all map configurations for all accounts.

Interface Type *[Administrator or IT Manager only]*

Sets the media type used for the line.

When to use it

- When Network Discovery does not recognize the type of interface for the line.
- When Network Discovery has set the wrong interface type for the line.

Effects

Changing interface type affects all map configurations for all accounts.

Limits

Network Discovery assigns a default duplex to each interface type. Full duplex and half duplex are listed separately.

Table 10: Interface types—half duplex

- ARCnet
- ISO 802.5r DTR
- HIPPI-800
- Asynchronous Protocol
- ISO 88024 Token Bus
- HIPPI-6400
- CATV Downstream interface
- ISO 88026 MAN
- IBM Multi-Protocol Channel Support
- Combat Net Radio
- Other
- IBM Twinaxial Data Link Control
- DVB-RCC Downstream Channel
- Proprietary Pt-Pt Wireless Interface
- IEEE 802.11 Radio LAN
- Ethernet 3Mbit
- Proteon 80Mbit
- Interleave Channel
- Fast Channel
- StarLan
- ISO 802.5 CRFP
- FDDI
- FibreChannel
- ARCnet Plus
- ISO 88023 CSMA/CD
- HIPPI
- Bisynchronous Protocol
- ISO 88025 Token Ring
- HSSI
- CATV Upstream interface
- LocalTalk
- IBM System 360/370 OEMI Channel
- DLSw - Data Link Switching
- Parallel Port
- IEEE 1394 High Performance Serial Bus
- DVB-RCC Upstream Channel
- Proteon 10Mbit
- IEEE 80212 100VG AnyLAN
- Ethernet CSMA/CD
- SDLC
- IP over Power Lines
- Fast Ethernet 100BaseT
- USB (Universal Serial Bus)
- ISO 802.5j Fiber Token Ring

Table 11: Interface types—full duplex

- AAL5
- Appletalk Remote Access Protocol
- Asymmetric Digital Subscriber Loop
- ATM (Cells)
- ATM DXI
- ATM Emulated circuit
- ATM Emulated LAN for 802.3
- ATM Emulated LAN for 802.5
- ATM FUNI
- ATM IMA
- ATM Logical Port
- ATM Sub Interface
- ATM Virtual Interface
- Avalon Parallel Processor
- Avici Composite Link Interface
- Basic Rate ISDN
- BBN Report 1822 - HDH
- BBN Report 1822 - VDH
- CATV MAC Layer
- CCITT G703 at 2Mbps
- CCITT G703 at 64Kbps
- CCITT V.11/X.21
- CCITT V.36
- CCITT V.37
- CCITT-ITU X.213
- CCITT-ITU X.29 PAD Protocol
- CCITT-ITU X.3 PAD Facility
- Channel
- Circuit Emulation Service
- Coffee Pot
- Data Communications Network
- DDN X25
- DS-0
- DS-0 Bundle
- DS-1
- DS-3/E-3
- DVB-RCC MAC Layer
- Dynamic Synchronous Transfer Mode
- E-1
- Encapsulation Interface
- EON (CLNP over IP)
- ESCON
- Ext Pos Loc Report Sys
- Fast Ethernet 100BaseFX
- Frame Forward Interface
- Frame Relay (DTE)
- Frame Relay Interconnect
- Frame Relay Service
- Gigabit Ethernet
- HDLC
- Hyperchannel
- IBM Common Link Access to Workstn
- IBM IP Over ATM
- IBM IP Over CDLC
- IBM StackToStack
- IBM VIPA
- IEEE 802.3ad Link Aggregate
- IP for APPN HPR in IP Networks
- IP Forwarding Interface
- IP Switching Objects
- ISDL
- ISDN and X.25
- ISDN S/T interface
- ISDN U interface
- ISO 88022 LLC
- LAPB
- LAPF
- Layer 2 Virtual LAN using 802.1Q
- Layer 3 Virtual LAN using IP
- Layer 3 Virtual LAN using IPX
- Link Access Protocol D
- MIO X.25
- Modem
- MPLS Tunnel Virtual Interface
- Multimedia Mail Over IP
- Multiprotocol Interconnect Over FR
- Multi-rate Symmetric DSL
- Myricom Myrinet
- NSIP (XNS over IP)
- PPP
- PPP Multilink Bundle
- Primary Rate ISDN
- Proprietary Connectionless Protocol
- Proprietary Multiplex
- Proprietary Pt-Pt Serial
- Proprietary Virtual/Internal
- Rate-Adapt. Digital Subscriber Loop
- Remote Source Route Bridging
- RFC1483 Multiprotocol Over ATM AAL5
- RFC877 X.25
- RS-232
- SIP (SMDS)
- SLIP
- SMDS DXI
- SMDS LCIP
- SNA X.25 QLLC
- Software Loopback
- SONET
- Sonet Path
- Sonet VP
- Spatial Reuse Protocol
- SS7 Signaling Link
- Symmetric Digital Subscriber Loop
- Transparent HDLC
- ULTRA
- V.35
- Very H-Speed Digital Subscrib. Loop
- Voice Encapsulation
- Voice Foreign Exchange Office
- Voice Foreign Exchange Station
- Voice Over ATM
- Voice Over Frame Relay
- Voice Over IP Encapsulation
- Voice recEive and transMit
- X.25 Hunt Group
- X.25 Multi-Link Protocol
- X.25 PLE

Related To change the duplex, see *Duplex Mode [Administrator or IT Manager only]* on page 226.

Alarm Type *[Administrator or IT Manager only]*

Sets the alarm type for the connection. The alarm type is normally associated with the interface type, but may be changed independently.

When to use it

When the default alarm type associated with the interface is inappropriate.

Effects

- Changing alarm type affects all map configurations for all accounts.
- Alarm types affects the thresholds for
  - maximum and typical MTU (maximum transmission unit)—that is, the largest packet or frame that the interface type permits (packet- or frame-based networks only)
  - broadcasts
  - errors
  - MTTR (alarm and warning thresholds; in hours)
- Collision thresholds are valid only when the alarm type is for an Ethernet half duplex connection (alarm types 3, 5, and 7)

Limits

Table 12: Alarm types

- No Alarms*
- Backup Line
- Generic HD
- Generic FD
- Ethernet 10< HD
- Ethernet 10< FD
- Ethernet 100 HD
- Ethernet 100 FD
- Ethernet 1000 HD
- Ethernet 1000 FD
- Token Ring
- FDDI HD
- FDDI FD
- 100VG AnyLAN
- Fibre Channel
- Computer Interfaces
- ATM (Cells) FD
- ATM (Frames) FD
- Low Speed Point to Point Serial HD
- Low Speed Point to Point Serial FD
- High Speed Point to Point Serial HD
- High Speed Point to Point Serial FD
- Low Speed Serial to SPN HD
- Low Speed Serial to SPN FD
- High Speed Serial to SPN HD
- High Speed Serial to SPN FD
- Low Speed Frame Relay FD
- High Speed Frame Relay FD
- Low Speed DSL FD
- High Speed DSL FD
- User Defined 1
- User Defined 2

* If you select “No Alarms”, Line Breaks will not be reported for the line.

Table 13: Abbreviations used in alarm types

Abbreviation	Expanded form
ATM	asynchronous transfer mode
DSL	digital subscriber line
FD	full duplex
FDDI	fiber distributed data interface
HD	half duplex
LAN	local area network
SPN	switched packet network

Table 14: Alarm type fields and values

Field	Values	Valid for
MaxMTUSizeBytes	53 | *1500* | 2112 | 4500 | *18000* | 65535	packet- or frame-based networks
TypicalMaxMTUSizeBytes	53 | *1500* | 2112 | *4470* | 9188 | 17966 | 65535	packet- or frame-based networks
UsageAlarmPercent	50 | 55 | 65 | 75 | 80 | 85	—
UsageWarningPercent	20 | 35 | 45 | 50 | 60	—
CollisionsAlarmSec	100	Ethernet Half Duplex
CollisionsWarningSec	50	Ethernet Half Duplex
BroadcastsAlarmSec	50	—
ErrorsAlarmSec	2	—
ErrorsWarningSec	1	—
MTTRAlarmHours	12 | 24 | 48	—
MTTRWarningHours	6 | 12 | 24	—
MTBFAlarmDays	180	—
MTBFWarningDays	365	—

Duplex Mode *[Administrator or IT Manager only]*

Sets the duplex to full or half. Full duplex allows for two-way communication over a line; half duplex permits only one-way communication.

When to use it When Network Discovery has set the wrong duplex.

Limits Full | half

Effects

- Duplex affects utilization statistics.
- Changing duplex affects all map configurations for all accounts.

Purge Port *[Administrator or IT Manager only]*

Removes the port from the device's model as created by Network Discovery.

Warning: This action cannot be undone.

Important: You are *not* making a physical change to the port. If you purge a port but the port is still operational, the port will be rediscovered and will reappear.

When to use it When a port has been removed from the network and you wish to update Network Discovery's representation of the device.

Effects

- Deletes the statistical history associated with the port. This in turn affects the graphs and reports for this port.
- Deletes the events associated with the port from the event log.
- breaks the connection on the port

Related

- To break a connection between ports, see *Break Connection [Administrator or IT Manager only]* on page 227.
- To purge an attribute, see *Purge Attribute [Administrator or IT Manager only]* on page 246.
- To purge a device, see *Purge [Administrator or IT Manager only]* on page 162 or *Purge device [Administrator or IT Manager only]* on page 202.

Create Connection *[Administrator or IT Manager only]*

Forces a new connection. You can create a connection to a real device or to a virtual device.

Tip: You can create a virtual device by creating a connection to a nonexistent virtual device.

Connections changes take effect at the end of the current sampling period.

Effects

Important: Do not create a connection to another real device except as a last resort. If you force a connection prematurely, you could slow Network Discovery down or even make it impossible for Network Discovery to correctly connect to your network. Never use forcing a connection as a quick fix.

Note: An exception: you may create connections to ports external to your network (for example, to your ISP) to ensure that the line break is reported.

- Forcing a connection affects all map configurations for all accounts.
- Forcing a new connection first breaks any existing connection.

When to use it

When Network Discovery has made incorrect assumptions about connectivity.

Break Connection *[Administrator or IT Manager only]*

Breaks an existing connection.

When to use it

When Network Discovery has made incorrect assumptions about connectivity.

Related

See also the Line Manager *Break Connection [Administrator or IT Manager only]* on page 238.

Refresh

Refreshes the contents of the panel.

Limits

Does not re-read the data in the panel from the network. Re-reads the data only from the Network Discovery database.

Print

Sends the contents of the panel to a printer attached to the management workstation.

Stop

Stops transfer of information from the Peregrine appliance to the Port Manager.

Text

Displays the contents of the Port Manager as text that can be copied and pasted.

Note: If the Statistics **Graph** panel is displayed, the Text button displays a text version of the Table, since there can be no text version of a graph.

Note: Not available to **Interface Rate**, **Interface Type**, **Alarm Type**, **Duplex Mode**, or **Connection**.

Note: May cause the panel to be refreshed with new data.

Procedural alert

To return to non-text mode, click the currently depressed button again.

Close

Closes the window and exits the Port Manager.

Port number

Allows you to select from the valid port numbers for this device.

Note: The number Network Discovery uses for the port may not match the physical port.

Port labelling standards for Cisco devices

Peregrine has adopted the following port labelling standards for Network Discovery's representations of Cisco devices.

Network Discovery checks the following MIB variable on each port.
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName
31.1.1.1.1

This MIB variable defines the relationship between the ifIndex and the representation of the actual physical port.

If a Cisco device MIB has the MIB variable, Network Discovery assigns a Cisco port label as well as the ifIndex. If the MIB does not have the variable, Network Discovery can use only the ifIndex to label ports. In general though, all Cisco devices have this MIB variable.

Network Discovery adds 1 to Cisco zero-based labelling

Cisco port labelling is "zero-based"; Port 0 is reported in the MIB. That means the information reported in the MIB is generally 1 less than the actual port label. Network Discovery corrects for this by adding 1 and represents the port correctly as Port 1.

If the MIB variable has the data "module/port" (5/1) then Network Discovery calls the corresponding port label module.port (5.1). Here is an example:

ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.13 = 5/1= Network Discovery label 5.1

In other words:

ifindex 13 contains 5/1 in the MIB so Network Discovery shows you a port index of 5.1

Network Discovery uses numbers to represent letter prefixes

If the MIB variable has letter prefixes, Network Discovery adds a prefix number to the label. The number comes from the IANA interface type list and is usually the interface type of the short form letters.

For example, any one of "Se", "Serial", "Hssi" or "Hs" may occur as prefixes in a MIB for a serial port. On encountering the prefix in the MIB, Network Discovery classifies the port as a proprietary point-to-point serial port and labels it "22".

Table 15: Port labelling standards

Code in the MIB	Definition	Network Discovery label
prefix	port description	port label assigned by Network Discovery
■ Se ■ Serial ■ Hssi ■ Hs	Proprietary Point to Point Serial	22
BR	a basic ISDN port	20
■ lo ■ Lo	to a loop back port	24
■ Fa ■ FastEthernet	Fast Ethernet (100BaseT)	62
ATM	ATM	37
■ Et ■ Ethernet	Ethernet	7
■ Gi ■ GigabitEthernet	Gigabit ethernet	117

Code in the MIB	Definition	Network Discovery label
■ To ■ TokenRing"	Token Ring	9
■ Fd ■ Fddi	FDDI	15

In the following example, “Se” in the MIB maps to “22” in Network Discovery. (Remember too that Network Discovery adds “1” to the 0/0 in the MIB so the resulting label is 1.1.)

ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.1 = Se0/0 = Network Discovery label 22.1.1

Table 16: More examples: how Cisco MIBs map to Network Discovery tables

Information in the MIB	Network Discovery label
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.2 = Fa0/1	62.1.2
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.3 = Fa0/2-	62.1.3
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.50 = Gi0/1	117.1.2
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.51 = Gi0/2	117.1.3

Frame Relay PVC ports or ATM Virtual Circuits (VC)

When Frame Relay PVC ports or ATM VC (Virtual Circuits) are assigned to the physical ports, the PVC or VC indexes are appended as a suffix to the Network Discovery port label. Here’s an example:

Se0/0 with iftype=22 plus PVC index=34 = Network Discovery label 22.1.1.34

Panel Elements

Common Elements

Certain elements are common to all Port Manager panels:

- 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. (In some cases, data may be shown in parentheses rather than with a gray background.) To change the time before data is considered stale, see *Account Properties* on page 282.
- A neutral signal light indicates that data is not available for a device or port.
- The final line on each panel is the date and time that the panel was refreshed. (This refers to rendering the panel itself, not when the data shown in the panel was last read.) This date can be useful for when you print a panel. To change the format of this date, see *Account Properties* on page 282.

Banner

The banner that appears at the top of all Port Manager panels consists of four elements.

Table 17: Port Manager banner

Element	Example	Notes
Device title and IP address	website.example.com / 192.168.96.1	■ see *Title* on page 232 ■ if the device title is the IP address, the IP address is shown once ■ if there is no IP address, only the device title is shown
Manager name	Port Manager	—
System name of Peregrine appliance	ExampleCorp	see *Appliance System Variables* on page 294
Web browser name	Netscape | Internet Explorer	—

Title

Options

The title displayed is associated with the device, not the port. The title is the first available of:

- user-assigned name
- Prime-assigned name
- device title chosen by the Network Discovery Administrator in **Administration** > **Display Preferences** > **Device Title Preference**; (see *Device Title Preference* on page 369). The Network Discovery Administrator can choose one or several of the following and choose their order too:
    - Asset Tag
    - BIOS Asset Tag
    - NetBIOS Name (scan)
    - Last Name
    - First name
    - Device-specific title
    - Domain name
    - NetBIOS name (network)
    - Operating system
    - Family
    - Model
    - Network function
    - System description
    - System name
    - System location
    - System contact
- IPv6 address
- IPv4 address
- MAC address including OUI
- MAC address (all-numeric)

Note: You cannot open the Port Manager from a virtual device.

Titles from the Prime configuration are inherited when you open your configuration. The only way to prevent the Prime title from being used is to assign a title yourself by using *Properties* on page 159. You cannot force the use of the default device title instead. (To determine the default title, see the *Diagnosis* panel of the Device Manager.)

13 Line Manager

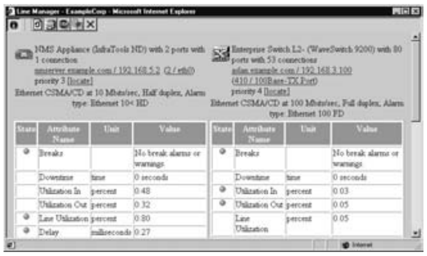
CHAPTER

The Line Manager has two modes, single line and multiple lines.

Figure 13-1: Line Manager modes

If the Line Manager window looks like this:

▶See *Single line* on page 235



NMS Appliance (InfraTools ND) with 2 ports with 1 connection
nmserver.example.com / 192.168.5.2 (2 / eth0)
priority 3 [locate]
Ethernet CSMA/CD at 10 Mbits/sec, Half duplex, Alarm type: Ethernet 10< HD

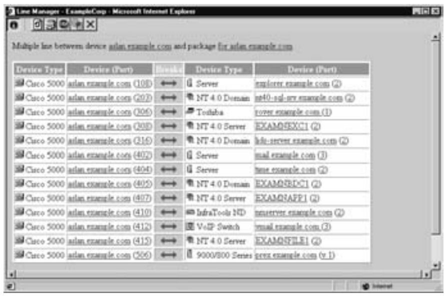
State	Attribute Name	Unit	Value
●	Breaks		No break alarms or warnings
	Downtime	time	0 seconds
	Utilization In	percent	0.48
	Utilization Out	percent	0.32
●	Line Utilization	percent	0.80
●	Delay	milliseconds	0.27

Enterprise Switch L2- (WaveSwitch 9200) with 80 ports with 53 connections
atlan.example.com / 192.168.3.100
(410 / 100Base-TX Port)
priority 4 [locate]
Ethernet CSMA/CD at 100 Mbits/sec, Full duplex, Alarm type: Ethernet 100 FD

State	Attribute Name	Unit	Value
●	Breaks		No break alarms or warnings
	Downtime	time	0 seconds
●	Utilization In	percent	0.03
●	Utilization Out	percent	0.05
	Line Utilization	percent	0.05

If the Line Manager window looks like this:

▶See *Multiple lines* on page 237



Multiple line between device atlan.example.com and package for atlan.example.com

Device Type	Device (Port)	Breaks	Device Type	Device (Port)
Cisco 5000	atlan.example.com (108)	⟷	Server	explorer.example.com (2)
Cisco 5000	atlan.example.com (203)	⟷	NT 4.0 Domain	nt40-sql-srv.example.com (2)
Cisco 5000	atlan.example.com (306)	⟷	Toshiba	rover.example.com (1)
Cisco 5000	atlan.example.com (308)	⟷	NT 4.0 Server	EXAMNEXC1 (2)
Cisco 5000	atlan.example.com (316)	⟷	NT 4.0 Domain	kdc-server.example.com (2)
Cisco 5000	atlan.example.com (402)	⟷	Server	mail.example.com (3)
Cisco 5000	atlan.example.com (404)	⟷	Server	time.example.com (2)
Cisco 5000	atlan.example.com (405)	⟷	NT 4.0 Domain	EXAMNBDC1 (2)
Cisco 5000	atlan.example.com (407)	⟷	NT 4.0 Server	EXAMNAPP1 (2)
Cisco 5000	atlan.example.com (410)	⟷	InfraTools ND	nmserver.example.com (2)
Cisco 5000	atlan.example.com (412)	⟷	VoIP Switch	vmail.example.com (3)
Cisco 5000	atlan.example.com (415)	⟷	NT 4.0 Server	EXAMNFILE1 (2)
Cisco 5000	atlan.example.com (506)	⟷	9000/800 Series	prex.example.com (v.1)

Introduction

Provides you with detailed information about the two devices on either side of a connection.

The line can be between:

- the ports on two known devices
- a port on a known device and an unknown port on a device
- unknown ports on two devices

Ways of opening

- From a map window, double-click a line.
- From a map window, point cursor at a line, and right-click.
- From a Service Analyzer path diagram, click on a line.
- Click a [line] hyperlink. Line hyperlinks appear in Manager panels.
- a report

Effects Selecting a line on the map opens either a single line window or a multiple line window.

Toolbar

The Line Manager has two panels. Its principal panel is About.

Table 1: Available toolbar buttons

Icon	Button name	Page	Virtual device
ⓘ	About	page 235	YES
	Break Connection [Administrator or IT Manager only]	page 238	YES

About

The About panel displays statistics for ports on both sides of a connection. This panel has two modes:

- *Single line*
- *Multiple lines* on page 237

Single line

The Line Manager shows two columns. In each column are a device and the relevant port for that device. If the Line Manager was opened by the Device Manager or Port Manager, the left column contains the device that was in context for the other Manager.

This panel is divided into two main sections:

- Heading
- State and Attribute Name (with Unit and Value)

Heading

Displays enough data to allow you to identify any device with which the port is associated.

Table 2: Heading elements

Element	Notes	Type
Icon	for a complete list, see Figure 10-5 and Figure 10-6 on page 161	all
Object type	for a complete list, see **Help** > **Device Types**	all
Device tag	see *Tag* on page 116	real
Port (optional)	the number that Network Discovery uses for the port may not match the physical port	real
Connections	includes user-assigned connections	all
Icon flag	appears if assigned by user	—
Object title	first title available; see *Title* on page 208; hyperlink to Device Manager	all
Title flag	appears if assigned by Prime configuration or user	all
Port title	port index and port description; hyperlink to Port Manager	all
Priority	see *Priority* on page 28	all
Priority flag	appears if assigned by Prime configuration or user	all
[locate] hyperlink	hyperlink to map window	all

Table 2: Heading elements (Continued)

Element	Notes	Type
Cloud number	created by Network Discovery or by an Administrator or IT Manager account user	virtual
Port properties (not labelled)	from the MIB, includes: ■ interface type ■ interface speed ■ duplex ■ alarm type (from the Network Discovery Rulebase)	real

Underneath the heading is a single line that explains how the connection was made. This is identical to the "Connection method" row in the Port Manager panel for *Diagnosis* on page 214.

State

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, displays alarms and warning signals even when the priority for the device (and its ports) is less than the minimum priority for a configuration.

A neutral signal light indicates that data is not available for a device or port.

Attribute name

Displays the current statistics for any attribute available.

These values are refreshed at the end of each poll cycle and may change each time they are viewed.

The metrics tables presented here is similar to the ones that would appear in the Device Manager and Port Manager's State panel (see page 182 and page 213) for each device port. The only difference here is the absence of the "value time column."

Note: It is important to understand that metrics for the two device ports will probably not match exactly. This is because the statistics for each device are not collected at the same time. Although there is rarely an exact match, the two sets of statistics should however be approximately equal, with in/out values reversed.

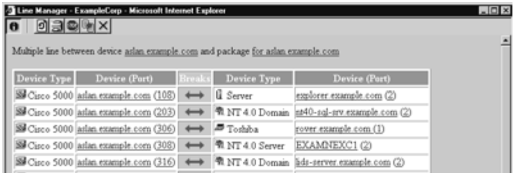
Multiple lines

The multiple line window opens when a line represents multiple connections between:

- two devices
- a device and a package
- two packages

If a package has a single external connection (that is, a single connection leading outside the package), the Line Manager opens in single line mode instead of in multiple line mode.

Figure 13-2: Multiple line window



Multiple line between device aslan.example.com and package for aslan.example.com

Device Type	Device (Port)	Breaks	Device Type	Device (Port)
Cisco 5000	aslan.example.com (108)	⟷	Server	explorer.example.com (2)
Cisco 5000	aslan.example.com (203)	⟷	NT 4.0 Domain	nt40-sql-srv.example.com (2)
Cisco 5000	aslan.example.com (306)	⟷	Toshiba	rover.example.com (1)
Cisco 5000	aslan.example.com (308)	⟷	NT 4.0 Server	EXAMNEXC1 (2)
Cisco 5000	aslan.example.com (316)	⟷	NT 4.0 Domain	lds-server.example.com (2)

The first line of a multiple line window tells you which objects the line connects. Click the hyperlink to open a Device Manager (if a device) or to open the map window (if a package).

All subsequent lines list the objects connected and their states. These lines are grouped by device, and the groups are sorted by port index number.

There are usually five hyperlinks for each entry:

- two hyperlinks to the Device Manager (one for each device on each side of the connection)
- two hyperlinks to the Port Manager (one for each port index on each side of the connection). If, however, the port is unknown, there will not be a hyperlink to a Port Manager.
- one hyperlinked arrow to a single-line window that connects two devices

The middle column contains colored arrows that both:

- link to a single-line window
- display the state of each line

If any Line Faults buttons are selected:

- the arrow will be in the alarm, warning, ok, or neutral colors, and the pop-text will reflect the state (not the color) of the line
- the column heading will be the name of the button (for example, “Errors”)

If no Line Faults buttons are selected:

- the arrow will be neutral color, and the pop-up text for the arrow will read “Idle”
- the column will have the heading “Line”

Break Connection *[Administrator or IT Manager only]*

Breaks an existing connection.

When to use it When Network Discovery has made incorrect assumptions about connectivity.

Related See also the Port Manager *Break Connection [Administrator or IT Manager only]* on page 227.

Refresh

Refreshes the contents of the panel.

Limits Does not re-read the data in the panel from the network. Re-reads the data only from the Network Discovery database.

Print

Sends the contents of the panel to a printer attached to the management workstation.

Text

Displays the contents of the Line Manager as text that can be copied and pasted.

Note: May cause the panel to be refreshed with new data.

Procedural alert

- To return to non-text mode, click **About** again.

Close

Closes the window and exits the Line Manager.

Panel Elements

Common Elements

Certain elements are common to most Line Manager panels:

- When data in a table has a gray background, the data shown is considered stale, since it was obtained before the beginning of your selected time period. (In some cases, data may be shown in parentheses rather than with a gray background.) To change the time before data is considered stale, see *Account Properties* on page 282.
- A neutral signal light indicates that data is not available for a device or port.
- The final line on each panel is the date and time that the panel was refreshed. (This refers to rendering the panel itself, not when the data shown in the panel was last read.) This date can be useful for when you print a panel. To change the format of this date, see **Administration** > **Account administration** > **Account properties**.

Banner

The banner that appears at the top of all Line Manager panels consists of three elements.

Table 3: Line Manager banner

Element	Example	Notes
Manager name	Line Manager	—
System name of Peregrine appliance	ExampleCorp	see *Appliance System Variables* on page 294
Web browser name	Netscape | Internet Explorer	—

14 CHAPTER

Attribute Manager

- To explore icon buttons in the toolbar menus, see:
  - Manager toolbar (page 242)
  - Statistics toolbar (page 245)
- To interpret data in the Attribute Manager window, see *Panel Elements* on page 248.

Introduction

1 Provides you with detailed history of an attribute associated with a device or a port.

Note: Virtual devices cannot have attributes.

Administrator or IT Manager: Also enables you to change the state of an attribute, and to change the way Network Discovery perceives an attribute.

Ways of opening

Click an attribute hyperlink from:

- the Device Manager State panel
- the Port Manager State panel
- the Line Manager About panel

Default panel

- *initial:* Configuration
- *subsequent:* from *Account Properties* on page 309

Toolbar

Availability of buttons in the Attribute Manager toolbar.

Table 1: Available toolbar buttons

Icon	Button name	Page
ℹ	Configuration	page 243
Σ	Statistics	page 245
🔍	Locate	page 246
🖥	Manage [Administrator or IT Manager only]	page 246
X	Purge Attribute [Administrator or IT Manager only]	page 246

Configuration

Identifies an attribute and presents details of its most recently observed state.

Heading

Table 2: Heading

Element	Notes
Icon	for a complete list, see Figure 11-5 and Figure 11-6 on page 205
Descriptive prefix	for example, “SNMP-managed device”
Device type	for a complete list, see **Help** > **Device Types**
Device tag	see *Tag* on page 116
No. of ports	the number Network Discovery uses for the port may not match the physical port
No. of connections	includes user-assigned connections
Icon flag	appears if assigned by an Administrator or IT Manager account user
Object title	first title available; see *Title* on page 208
Address	IP address; does not appear if identical to object title
Port no./ description	number of port / description of port
Title flag	appears if assigned by Prime configuration or user
Priority	see *Priority* on page 28
Priority flag	appears if assigned user

Identity

Table 3: Identity

Element	Notes	Optional
Name	for a complete list, see **Help** > **Supported Device/Port Attributes**	NO
Description	there can be multiples of an attribute (for example, disk, CPU, memory, toner)	YES
Units	varies according to the attribute, for example, time, percent, bytes/sec., frames/sec., milliseconds, days and hours, gigabytes. Not applicable for Breaks	YES
Maximum value	—	YES
Alarm threshold	available only for those attributes tracked on the Health Panel	YES
Warning threshold		YES
State		YES

Table 3: Identity (Continued)

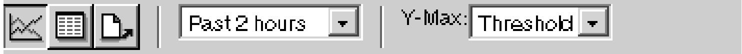
Element	Notes	Optional
Value	—	NO
Value time	—	NO

Statistics

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.

Note: "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.

Figure 14-1: Statistics toolbar



Options

Graph

Statistics for the past 48 hours are averaged every 5 minutes, statistics for the past 31 days are averaged every hour, and statistics for the past 365 days are averaged every day.

Whenever a graph contains multiple averages, the data is adjusted to the lowest common denominator. For example, a graph of the past 7 days contains only one-hour data points. The data points used are indicated on the graph.

Gray portions of the graph indicate that data was not available for a period. Lighter gray is used for unavailable average data, darker gray for unavailable peak data. Also shown on the graph are horizontal lines representing alarm and warning thresholds.

Table

Average in and average out are the sum of all the values for each port of the device. For example, if a concentrator has 10 ports, the average output is ten times the output on each port.

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 Network Discovery.

Periods

Daily views have statistics averaged every 5 minutes. Monthly views have data averaged every hour. Yearly views have data averaged every day.

Limits

- *period:* 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:* Threshold Max | Data Max | Attribute Max

Locate

Highlights in a map window the location of the device to which this attribute refers.

If you have a map open

▶ Click **Locate**.

A map window opens. Within the window, the device have a purple rectangle drawn it.

If the window containing the device was already open, that window becomes the front-most window, and the window scrolls so that the highlighted icon can be seen.

Manage *[Administrator or IT Manager only]*

Manages the attribute.

Examples: In the case of ports, Administrative Status can be turned on or off. In the case of the Bridge Aging Interval, the length of the interval can be changed.

Limits

- Available only when Network Discovery has a write community string for the attribute.
- Not all attributes can be managed.

Purge Attribute *[Administrator or IT Manager only]*

Removes an attribute and its historical statistics from the Network Discovery database.

Warning: This action cannot be undone.

Important: You are *not* making a physical change. If you purge an attribute but the attribute is still present—that is, still associated with a device or port that is still present in your network—Network Discovery will discover the attribute and the attribute will reappear.

When to use it

- When an attribute is no longer associated with a device or port.
- When you no longer wish to retain or examine the history of an attribute.

Related

- To purge a device, see *Purge [Administrator or IT Manager only]* on page 162.
- To purge a port, see *Purge Port [Administrator or IT Manager only]* on page 226.

Refresh

Refreshes the contents of the panel.

Limits

Does not re-read the data in the panel from the network. Re-reads the data only from the Network Discovery database.

Print

Sends the contents of the panel to a printer attached to the management workstation.

Text

Displays the contents of the Attribute Manager panel as text that can be copied and pasted.

Note: If the Statistics **Graph** panel is displayed, the Text button displays a text version of the Table, since there can be no text version of a graph.

Note: May cause the panel to be refreshed with new data.

Procedural alert

To return to non-text mode, click the currently depressed button again.

Close

Closes the window and exits the Attribute Manager.

Panel Elements

Common Elements

Certain elements are common to all Attribute Manager panels:

- 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. (In some cases, data may be shown in parentheses rather than with a gray background.) To change the time before data is considered stale, see *Account Properties* on page 282.
- A neutral signal light indicates that data is not available for a device or port.
- The final line on each panel is the date and time that the panel was refreshed. (This refers to rendering the panel itself, not when the data shown in the panel was last read.) This date can be useful for when you print a panel. To change the format of this date, see *Account Properties* on page 282.

Banner

The banner that appears at the top of all Attribute Manager panels consists of four elements.

Table 4: Attribute Manager banner

Element	Example	Notes
Attribute name	Administrative Status	—
Device title and IP address	website.example.com / 192.168.96.1	■ see *Title* on page 249 ■ if the device title is the IP address, the IP address is shown once ■ if there is no IP address, only the device title is shown
Manager name	Attribute Manager	—
System name of Peregrine appliance	ExampleCorp	see *Appliance System Variables* on page 294
Web browser name	Netscape | Internet Explorer	—

Title

Options

The title for a device (real or virtual) is the first available of:

- user-assigned name
- Prime-assigned name
- *virtual devices only:* Network Discovery generated name
- a device title chosen by the Network Discovery Administrator in **Administration** > **Display Preferences** > **Device Title Preference**; (see *Device Title Preference* on page 369). The Network Discovery Administrator can choose one or several of the following and choose their order too:
  - Asset Tag
  - BIOS Asset Tag
  - NetBIOS Name (scan)
  - Last Name
  - First name
  - Device-specific title
  - Domain name
  - NetBIOS name (network)
  - Operating system
  - Family
  - Model
  - Network function
  - System description
  - System name
  - System location
  - System contact
- IPv6 address
- IPv4 address
- MAC address including OUI
- MAC address (all-numeric)

Titles from the Prime configuration are inherited when you open your configuration. The only way to prevent the Prime title from being used is to assign a title yourself by using *Properties* on page 159. You cannot force the use of the default device title instead.(To determine the default title, see the *Diagnosis* panel of the Device Manager.)

15 CHAPTER

Service Analyzer

- For information about identifying the endpoints of the path, see *Query* on page 252.
- For information about analyzing results—path diagram, end-to-end analysis, and network analysis—see *Results* on page 253.

Introduction

Provides you with detailed information about the path between two objects.

The state of a path is useful when you are searching for the source of a problem and when you are attempting to determine the capacity of a path for a specific service, such as voice over IP. Since the available information spans yesterday and today, you can use the Service Analyzer to determine the source of problems that are no longer active.

Ways of opening

- From the main Toolbar, click the **Service Analyzer** button.
- From a map window or the Health Panel: Click the **Tools** menu, then click **Service Analyzer**.
- From a map window: Click the **Object** menu, then click **Analyze Services**.
- From the Device Manager, click **Service Analyzer**.

Query

The query window contains a single panel and two search boxes. Each box searches for a device based on its name, title, or address.

Limits

- The device must be on the Network Map.
- *Input:* “localhost” | “nmc” | MAC address | IPv4 address | IPv6 address | domain name | Prime-assigned title | user-assigned title | asset tag | NetBIOS name

Procedural alerts

- To find the Peregrine appliance, enter “nmc” or “localhost”.
- To find multiple devices in the Network Discovery ™ database, enter the first few letters of a title or the first number of an address. You are provided with a list box for each device that returned a multiple result. This allows you to select the desired device and proceed with the analysis.

Important: All multiple results are based on the device title. Example: If you enter “192.168.2.”, you do not find all devices 192.168.2.0–192.168.2.255. You find only devices with “192.168.2.” in the title. If the device with IP address 198.168.2.55 takes it title from its domain name, that device is not found.

Results

The results window contains a single panel and two list boxes, one for analysis panels, and one for paths.

Content

The first list box determines the content of the main Service Analyzer panel.

Each panel is intended to indicate the availability or stability of a path.

Table 1: Analysis panels

Group	Analysis panel	Purpose
—	Path Diagram	Displays the path between two devices and the states of devices and lines in that path
End to end Analysis	Service levels (all paths)	■ path number in use yesterday and today ■ delay (end to end) ■ packet loss (end to end) ■ jitter (end to end)
	Traffic levels (all paths)	■ peak utilization ■ peak broadcasts ■ peak collisions ■ peak errors
Network Analysis	Availability	Whether a path was up or down; for devices and ports.
	Transit Delay	Delay in milliseconds; for ports
	Packet Loss	Packet loss in percentage; for devices
	Line Utilization	Utilization in percentage; for ports, bi-directional
	Transit Jitter	Jitter (change in delay) in milliseconds; for ports, bi-directional
	Packet Broadcast	Broadcasts in frames/sec.; for ports, bi-directional
	Packet Collision	Collisions per seconds; for ports
	Packet Error	Errors in frames/sec.; for ports

Default

Path Diagram

Path

The second list box displays the alternate paths available between the two end devices. If there only a single path, as frequently occurs in many networks, it will be the only choice.

The percentage indicates how frequently a path was taken. If there is a single alternative and yet the percentage is less than 100, it usually indicates a device in the path was off or broken for some time over the preceding 48 hours.

Path Diagram

The path diagram presents devices and lines. Packages are not shown.

Device state is indicated by the color of its square background. All devices have a state, not just those equal to or above the minimum priority.

Line state is indicated by line color. The thickness of a line reflects its capacity. For example, a 100 Mbit/sec. line is thicker than a 10 Mbit/sec. line.

To focus on a specific device, click its icon to open a Device Manager. To focus on a line, click the line to open a Line Manager.

If any problems are detected on the path, they are summarized in a table underneath the path diagram.

Table 2: Problems detected on the path

Column	Notes	Example
State	—	—
Device (Port)	hyperlinked to Device Manager and Port Manager	rbuffin.example.com (1)
Attribute with Problem	■ attribute name ■ threshold (if applicable)	Errors In exceeds threshold of 2 frames/sec.
Value	■ Broadcasts | Errors: frames per second ■ Utilization | Packet Loss: percentage ■ Delay: response time in milliseconds ■ Collisions: collisions per second ■ Line Breaks | Device Breaks: no value shown	2.07 frames/sec.

Default

- *alarm color:* red
- *warning color:* yellow
- *OK color:* green

End to End Analysis

The focus of this section is on the entire path, end to end. The path selected in the *Path* list box is not relevant, and does not affect the display.

Service levels

The first graph displays the alternate (simultaneous) paths being used for a 48-hour period, today and yesterday. Even when there is only a single alternative, this graph shows when that path was available.

This graph is not reliable when Network Discovery is still determining connectivity between devices. It may indicate non-simultaneous paths, including paths that no longer exist.

The remaining graphs display delay, packet loss, and jitter across the entire path; for. today and yesterday, across the entire path.

Traffic levels

All graphs display traffic levels for a 48-hour period, today and yesterday, across the entire path.

Network Analysis

The focus of this section is on the elements that make up the path: devices and ports. Device titles are hyperlinked to the Device Manager; port numbers or descriptions are hyperlinked to the Port Manager.

For Availability, the graph displays whether the path was up or down over a 48-hour period, today and yesterday. For all panels except Availability, the graphs shown the peak statistic for the previous 48 hours.

For Availability, Packet Collision and Packet Error, graphs are shown both for devices and the ports on those devices. The inbound port is shown, then the device, then the outbound port. (The device at the start of the path does not show an inbound port; the device at the end does not shown an outbound port.) Every step along the path is clearly indicated.

For Transit Delay and Transit Jitter, graphs are shown for inbound and outbound ports.

For Packet Loss, graphs are shown for all devices on the path.

For Line Utilization and Packet Broadcast, there are a possible four graphs per device. Graphs for the inbound and outbound ports of a device are shown, and for each port, utilization to and back are shown.

Refresh

Refreshes the contents of the panel.

Limits Does not re-read the data in the panel from the network. Re-reads the data only from the Network Discovery database.

Print

Sends the contents of the panel to a printer attached to the management workstation.

Text

Note: This button is not available to Service Analyzer.

Displays the contents of the active window as text that can be copied and pasted.

Close

Closes the window and exits the Service Analyzer.

CHAPTER

16 Events Browser

- To explore icon buttons in the toolbar menu, see *Toolbar* on page 260.
- To interpret data in the Events Browser window, see *Event Entry* on page 259.
- To interpret data in the Aggregate Events Browser window, see *Aggregate Events Browser* on page 262.

Introduction

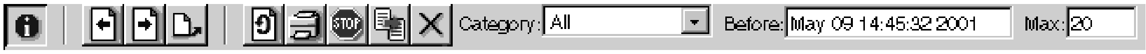
The Events Browser lists all events logged by Network Discovery that occurred in the network over a specified period. The most recent events are listed first.

An event is a transition between states: OK to alarm, OK to warning, warning to alarm, and so on. A transition is based on *Alarm Thresholds…* on page 142.

Event categories correspond to line and device fault category button on the Health Panel. In addition, there are "info" events: add and delete.

Note: The window is not automatically updated to reflect new events.

Table 1: Events Browser toolbar



Category: All

Before: May 09 14:45:32 2001

Max: 20

Limits

- 45 days or 500,000 events (whichever is less)

Important: The Events Browser view is not intended to be the same as the Health Panel fault events.

- There are two main reasons that the Events Browser does not match the Health Panel:
  - The Events Browser depends on the events log. The events log is created by four default "log-events" filters:

- email-system-device (node)
- email-system-line (port)
- log-events-device (node)
- log-events-line (port)
- Event filters are maintained by the Network Discovery Administrator or by other Administrator or IT Manager accounts. See *Event Filter Configuration* on page 337.
- The Events Browser is based on the Prime configuration and its device priorities.

Ways of opening

- From the main Toolbar, click the **Events Browser** button.
- From a map window or the Health Panel: Click the **Tools** menu, then click **Events Browser**.

Related

- To view only events specific to a device, see Device Manager *Events* on page 190.
- To view only events specific to a port, see Port Manager *Events* on page 219.
- To receive e-mail or pages about events, see *Account Properties* on page 282.
- Administrator: To change the data collected for display, modify the filters (see *Modify a Filter* on page 341).

Event Entry

Each row in the Events Browser window contains the following columns.

Table 2: Data in Events Browser table

Data	Limits/Options	Notes
Date/Time	—	The time the event was generated.
State	alarm | warning | OK | neutral | info	signal light
Category	Line Breaks | Utilization | Delay | Collisions | Broadcasts | Errors | Device Breaks | Packet Loss | Adds | Deletes	—
Priority	1–6	—
Device type	see *Device identification* on page 26	small device icon and tag
Device (Port)	—	■ device title* (maximum 30 characters)—hyperlinked ■ port (in parenthesis)—hyperlinked **Note:** If the traffic can be identified as inbound or outbound, this will also be noted.
Value	—	■ Broadcasts | Errors: frames per second ■ Utilization | Packet Loss: percentage ■ Delay: response time in milliseconds ■ Collisions: collisions per second ■ Line Breaks | Device Breaks: the time the Break is thought to have occurred.

* If no device title can be determined (as in the case where a device has a neither an IP address nor a MAC address), the Events Browser displays "[Unknown]".

Note: The priority for each entry is based on the Prime configuration.

Broadcast warnings are not logged, due to the potentially very high number of events. Broadcast alarms are logged.

Banner

The banner that appears at the top of the Events Browser panel consists of three elements.

Table 3: Events Browser banner

Element	Example	Notes
Browser name	Events Browser	—
System name of Peregrine appliance	ExampleCorp	see *Appliance System Variables* on page 294
Web browser name	Netscape | Internet Explorer	—

Toolbar

Events

Updates the window with the most recent events.

Older

Updates the window with earlier events, relative to currently displayed events.

Limits 45 days ago (or 500,000 events, whichever is less)

Related

- To change the number of line on a screen, see *Max.* on page 262
- To move to a specific, absolute time and date, see *Before* on page 262.

Newer

Updates the window with later events, relative to currently displayed events.

Limits current time

Related

- To change the number of line on a screen, see *Max.* on page 262.
- To move to a specific, absolute time and date, see *Before* on page 262.

Export

Exports selected events to a Comma Separated Value (CSV) file or XML file.

Table 4: Export defaults

	Limits	Default
From	January 1, 1970–December 31, 2037	—
To	January 1, 1970–December 31, 2037	—
Category	All | Line Breaks | Utilization | Collisions | Broadcasts | Errors | Device Breaks | Packet Loss | Adds | Deletes	current selection
Max	1–1000	1000

Refresh

Refreshes the events shown.

Limits Does not re-read the data in the panel from the network. Re-reads the data only from the Network Discovery database.

Print

Prints the events in the current window.

Text

Displays the contents of the Events Browser as text that can be copied and pasted.

Note: May cause the panel to be refreshed with new data.

Procedural alert To return to non-text mode, click **Events**.

Close

Closes the window and exits the Events Browser.

Category

Selects the category of events for display so that you can focus on a specific event type.

Table 5: Classes of events

Class	Category	Explanation	Notes
alarm	Breaks | Packet Loss | Utilization | Collisions | Broadcasts | Errors	alarm state (alarm, warning, or ok) of device or port changed	—
info*	Adds	device was added to the Network Map	not the same as when the device was discovered
	Deletes	device was removed from the Network Map	a device is removed when it is automatically placed in the trash by Network Discovery—see *Expiry* on page 352

* Info events are not sent to the Health Panel.

Limits All | Breaks | Packet Loss | Utilization | Collisions | Broadcasts | Errors | Adds | Deletes

Default All

Before

Set the time and date for the first entry for this window absolutely.

Limits

- *input*: January 1, 1970–December 31, 2037
- *display*: 45 days ago–current time

Default

Current time

Related

To move a screen at a time, relative to currently displayed events, see *Newer* on page 260 and *Older* on page 260.

Max.

Set the maximum number of events per window.

Limits

1–100

Default

20

Aggregate Events Browser

There is just one difference between the Events Browser and the Aggregate Events Browser. When a information for a device comes from a remote Peregrine appliance, (or more than one) the device title has a suffix "[via <Peregrine appliance name>]" for all appliances supplying the device.

Event Entry

Each row in the Aggregate Events Browser window contains the same columns as described in *Data in Events Browser table* on page 259.

Note: The priority for each entry is based on the Prime configuration.

Broadcast warnings are not logged, due to the potentially very high number of events. Broadcast alarms are logged.

17 Find

CHAPTER

Locates a device or a specific port of a device, and opens a Device Manager or Port Manager as appropriate.

There are three options:

Table 1: Find options

Panel	Searches
Device on page 264	■ address ■ title ■ asset tag
Port on page 265	■ number ■ description
Advanced on page 266	■ Network Discovery Rulebase ■ SNMP MIB

If you have a map open, Network Discovery locates a found device in the map window.

Ways of opening

- From the Toolbar, click the **Find** button.
- From the Health Panel or a map window, click the **Tools** menu, then click the **Find** command.
- From a map window, press Control-F.

Related

To find the path between two devices, see *Chapter 15, Service Analyzer*.

Device

Searches for a device based on its name, title, address, NetBIOS name, or asset tag.

The search stops at the first successful category.

> Example: Once an IP address has been found, Network Discovery does not search domain names and user-assigned titles.

Table 2: Device search results

If the numberof devices found is	Network Discovery does this:	You do this:
0	displays the message “not on map”	try entering the name again
1	opens a Device Manager	—
2–35	displays a list of all results	click the linked title of one device in the list to go to the Device Manager
36 or more	displays a list of the first 35 results and a message that some results are not displayed	■ click the linked title of one device in the list to go to the Device Manager ■ narrow your search and try entering the device again

Limits

- *Input:* “localhost” | “nmc” | MAC address | IPv4 address | IPv6 address | domain name | Prime-assigned title | user-assigned title | asset tag | NetBIOS name (network) | NetBIOS name (scan)
- *Output:* 0–35 results

Procedural alerts

- To find the Peregrine appliance, enter “nmc” or “localhost”.
- To find multiple devices in the Network Discovery database, enter the first letter of a title or the first number of an address.

Important: Only the options that have been selected in **Administration** > **Display Preferences** > **Device Title Preferences** affect the title search. For example, if you ask Network Discovery to search for devices with the Last Name “Tremblay”, but the Last Name option has not been selected, the search will fail even if the device is on the Network Map.

Important: All multiple results are based on the device title. Example: If you enter “192.168.2.”, you will not find all devices 192.168.2.0–192.168.2.255. You will only find devices with “192.168.2.” in the title. If the device with IP address 198.168.2.55 takes it title from its domain name, that device will not be found.

Port

Searches for a specific port of a device.

Table 3: Port search results

If the number of ports found is	Network Discovery does this:	You do this:
0	opens a Device Manager	—
1	opens a Port Manager	—
2–35	displays a list of all results (multiple devices, or multiple ports on a device)	■ click the linked title of one port in the list to be taken to the Port Manager ■ click the linked title of the device to be taken to the Device Manager
36 or more	displays a list of the first 35 devices and a message that some devices are not displayed	■ click the linked title of one port in the list to be taken to the Device Manager ■ narrow your search and try entering the port again

Limits

Input

- Port number
- Port description

Advanced

Searches for a device based on the contents of its SNMP MIB or Rulebase data.

Table 4: Advanced device search results

If the number of devices found is	Network Discovery does this:	You do this:
0	—	try entering the name again
1	opens a Device Manager	—
2–35	displays a list of all results	click the linked title of one device in the list to be taken to the Device Manager
36 or more	displays a list of the first 35 results and a message that some results are not displayed	click the linked title of one device in the list to be taken to the Device Manager~narrow your search and try entering the device again

Options

- Family | Model | Operating System | Application | SNMP Description | SNMP Contact | SNMP Name | SNMP Location
- Begins with | Ends with | Contains | Exact match | Match with wildcards | Match using a regular expression

Table 5: Wildcard characters

Option	Purpose	Example
?	Any single character	“gr?y” finds “gray” and “grey”
*	Multiple characters	“E*t” finds “Ethernet”

Note: Searches are not case-sensitive.

The “exact match” is inexact—case is not matched.

The “regular expression” is irregular—case is not matched.

Limits

- The device has to be on the Network Map.
- *Output:* 0–35 results

Defaults

- “Model”
- “contains”

Refresh

Refreshes the contents of the Find window.

Print

Sends the contents of the Find results panel to a printer attached to the management workstation.

Text

Note: This button is not available to Find.

Displays the contents of the active window as text that can be copied and pasted.

Close

Closes the window and exits the Find window.

18 Reports

CHAPTER

Network Discovery reports comprise the following groups:

- *Executive/Summary Network Reports* on page 271
- *WAN Reports* on page 273
- *LAN Reports* on page 274
- *Device Reports* on page 275
- *Support Reports* on page 276

Aggregator reports

The Aggregator has the same categories of reports that a single-appliance has.

Report periods

There are two types of report, summary and detail. Both report types have a different group of reporting periods.

Table 1: Reporting period groups for summary and detail

Summary	Detail
Today	All Periods*
Last 7 Days	Yesterday
Last Week	Last 7 Days
This Month	Last Week
Last Month	Last Month

* All periods in this group.

Table 2: Reporting periods

Period	Contents	Generated	Summary	Detail
Today	data for today and yesterday	each hour*	YES	—
Yesterday	data for the previous 24 hours	each day after midnight	—	YES

Table 2: Reporting periods (Continued)

Period	Contents	Generated	Summary	Detail
Last 7 Days	data for the previous 7 days, starting yesterday (not including today)	each day after midnight	YES	YES
Last Week	data for the previous week (weeks begin each Monday)	each Monday	YES	YES
This Month	data for the days in the current month, starting yesterday (not including today)	each day after midnight	YES	—
Last Month	data for the previous calendar month	on the first day of each month	YES	YES

* For a restricted period: 0600–2000 (6 AM–8 PM).

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: Examples for mean and peak values

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. A report for “Last 7 Days” takes samples every hour.

Executive/Summary Network Reports

Note: All reports will reflect the Prime map configuration and its packaging.

Table 4: Executive/Summary Reports reports

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	list
	Resource Managed Devices Inventory	list
	Resource Inventory and Usage	table
	Frame Relay PVC Inventory	table
	Possible Modems Report	list
	Underutilized Equipment	table
Performance Summaries	Network Summary Reports	line/bar graphs
	WAN Summary Reports	line/bar graphs
	Frame Relay Summary Reports	line/bar graphs
	DSL Summary Reports	line/bar graphs
	Point to Point Summary Reports	line/bar graphs
	Serial to SPN 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
Fault Summaries*	All Faults	table
	Line Breaks	table
	Line Utilization*	table
	Delay	table
	Collisions	table
	Broadcasts	table
	Errors	table
	Device Breaks	table
	Packet Loss	table

Table 4: Executive/Summary Reports reports (Continued)

Folder	Report	Type
Network Wide	Network Availability	line/bar graphs
	Mean Network Utilization	line/bar graphs
	Peak Network Utilization	line/bar graphs
	Mean Network Throughput	line/bar graphs
	Peak Network Throughput	line/bar graphs
	Inventory	list
	Availability Details	table
	Utilization Details	table

* Line fault reports include connected lines only.

Performance Summaries

These folders contain the following periods:

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

Fault Summaries

These folders contain the following periods:

- All Periods
- Yesterday
- Last 7 Days
- Last Week
- Last Month

Network Wide

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

- All Periods
- Yesterday
- Last 7 Days
- Last Week
- Last Month

WAN Reports

Note: All reports will reflect the Prime map configuration and its packaging.

There are two report structures for WAN Reports:

- Frame Relay folder
- all other folders

Table 5: Frame Relay reports

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
Detail Details

In Table 6, <*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)

Table 6: All other WAN Reports

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

Note: All reports will reflect the Prime map configuration and its packaging.

In Table 7, <*LAN_type*> stands for one of the following:

- LAN Backbone
- FDDI
- Token Ring

Table 7: LAN Reports

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	
Inventory	table
Availability Details	table
Utilization Details	table

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

- All Periods
- Yesterday

- Last 7 Days
- Last Week
- Last Month

Device Reports

Note: 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

Table 8: Device Reports

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

The Resource Managed folders contain the following:

- Inventory
- All Periods
- Yesterday
- Last 7 Days
- Last Week
- Last Month

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

Note: The Web Server Availability reports will reflect the Prime map configuration and its packaging.

Support Reports

Support reports include exceptions, which list any network-standard problems that could interfere with Network Discovery operation, and ways to document your network.

Table 9: Support Reports

Report Title	Details
Exceptions Summary	—
Exceptions	—
Device Inventory Export	—

Microsoft Word documents

Network Discovery comes with two documents for Microsoft Word that allow you to print reports with graphs of your network. The first document is a example report framework for the intermediate Microsoft Word user. To use it, you use cut and paste to rearrange the built-in graphs. The second document is a report template for the advanced Microsoft Word user. To use the second document, you should be comfortable with Word field codes and macro substitution.

Each document contains links to an Network Discovery graph on your Peregrine appliance. Once you customize the report with the name of your Peregrine appliance, you can easily update the graphs—to present at weekly meetings, for example.

Compatibility

Compatible with:

- Microsoft Word 97
- Microsoft Word 2000

Setup

The exact steps for setting up Microsoft Word to use the Network Discovery templates are described in the *User Guide.* In brief:

To install the Network Discovery templates for Microsoft Word:

Step 1 Find out where Microsoft Word keep its templates.

Step 2 Get the templates from the Peregrine appliance.

From the Reports menu, click the **Support** folder.

Step 3 Download the templates into the Microsoft Word template directory.

Step 4 Start Microsoft Word.

If Microsoft Word is already running, quit it and restart it.

Example report framework

The example report includes several graphs. You can rearrange these graphs, and delete those you don’t want. You can also customize the text of the report. We’ve tried to make it easy to use your name and company information throughout the report, and encourage you to customize it.

Because the graphs are actually linked to your Peregrine appliance, you can easily retrieve updated graphs. When you open the document, the graphs are automatically updated. You can also request a manual update.

The exact steps to request a manual update are described in the *User Guide*.

Report template

When using the report template, you must write a shortcut that automatically creates the necessary field codes for Microsoft Word’s INCLUDEPICTURE feature.

First, you create a document from our template:

1. From the **File** menu, click **New**.
2. Click the **General** tab.
3. Click the document labelled “SumRepUpdate.dot”.

Note: If you don’t see “SumRepUpdate.dot”, you may have skipped the *Setup* on page 277.

Next, you type the shortcut for the graph that you want to appear at that point in the Word document.

Graph shortcut

Instead of typing the exact URL for the graph stored on your Peregrine appliance, you type a shortcut that is automatically translated into the exact URL that INCLUDEPICTURE requires. The shortcut takes this form:

```
?graph(group,attr,stat,period,legend)?
```

Spaces are permitted between each element, but not within elements.

Once you have typed the shortcut into the template, you run a pre-recorded macro to translate the shortcut into a field code loads a fresh graph right from the Peregrine appliance.

To translate a shortcut:

1. Select the shortcut.
2. Do one of the following
   a. From the **Tools** menu, click **Macro**, then click **Macros**.
   b. Press Alt-F8.
3. Select the “SumRepUpdate” macro, then click **Run**.

When you open a document created using the template, the graphs are automatically updated.

group

Selects the group of line types for the graph.

Options

Table 10: *Parameters for group*

Parameter	Description
atmc	ATM (cell) lines
atmf	ATM (frame) lines
dsl	digital subscriber lines
fddi	FDDI
frm	frame relay lines
lanbb	LAN backbone
net	all lines
point	point to point lines
sspn	serial to service provider network lines
token	token ring
wan	all WAN lines (includes frm, atmc, point, sspn, dsl)

attr

Selects the attributes for the summary statistic.

Options

Table 11: Parameters for attr

Parameter	Description	Notes
avail	availability	If you choose avail, the parameter for stat is ignored.
util	utilization	—
vol	volume per second (throughput)	—

stat

Selects the statistical function. Not relevant when attr = avail.

Options

Table 12: Parameters for stat

Parameter	Description
mean	mean (average) values are plotted for each interval
peak	peak (highest) values are plotted for each interval

period

Selects the period over which the data will be graphed. (For details, see Table 13.)

Options

Table 13: Parameters for period

Parameter
today
thisweek
lastweek
thismonth
lastmonth

legend

Toggles whether create a legend for the graph.

Options

Table 14: Parameters for legend

Parameter	Description
yes	Create legend.
no	Don’t create legend.

19 CHAPTER Administration for IT Employee and IT Manager Accounts

Demo: You cannot perform any administration.

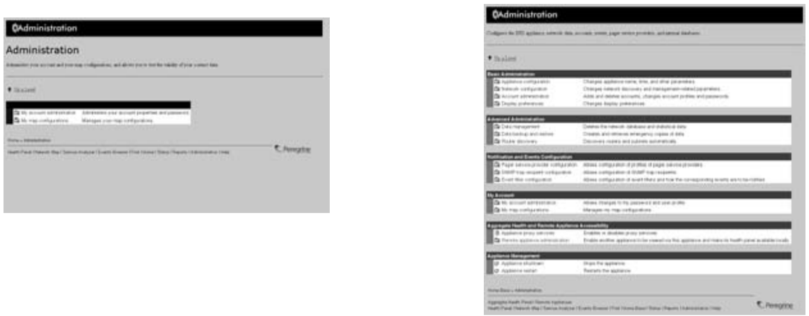
Figure 19-1: The two different Administration menus

If your menu looks like this:

▶Consult this chapter.

If your menu looks like this:

▶See *Chapter 20, Administration for Administrator Accounts*.



Enables a user to administer his or her own account. Also includes facilities to test the contact data the user provided to Network Discovery.

The Administration menu also allows IT Employee and IT Manager users to manage their own map configuration files.

My Account Administration

Account Properties

These settings allow you to customize how you interact with Network Discovery.

Options

Table 1: Account properties options

Option	Setting	Limits	Default
Name*		■ *valid characters:* A–Z, a–z, 0–9, - *(hyphen)*, _ *(underscore)*, *(space)* ■ *length of input:* 0–40 characters	—
Allow others to copy map configurations		Yes | No	No
Receive status e-mail		Yes | No	No
Append IP address		Yes | No	No
Visible URLs		Yes | No	No
Visible borders for text tables		Yes | No	No
Color alternate table rows		Yes | No	Yes
Highlight table rows		Yes | No	No
Visible navigation bar		Yes | No	No
Time before marking statistic as stale		10 minutes to 35 days	2 hours
Long date format		See Table 2 on page 284	%A, %B %e, %Y %T %Z
Short date format		See Table 2 on page 284	%Y-%m-%d %R
Inline help format		all | short	all
Default Device Manager panel		Configuration | State | Statistics | Ports | Events| Diagnosis | IP Ping | Traceroute | SNMP Ping | DNS Query | Update Model	State
Default Port Manager panel		Configuration | State | Diagnosis | Statistics | Events	State
Default Find panel		Device | Port | Advanced	Device
Default Attribute Manager panel		Configuration | Statistics	Configuration
Default Device Manager Ports panel selection	Selection	see *Device Manager Ports Display Preferences* on page 376	Status
	Increment	1–1000	24
Default Events Browser selection	Selection	All | Line Breaks | Utilization | Delay | Collisions | Broadcasts | Device Breaks | Packet Loss | Adds | Deletes	All
	Increment	1–1000	20

* Do not confuse this with the account name (login name).

Name

Helps you identify your account. Visible only in the status window of your Toolbar, in **Status** > **Network Map Sessions**, and to an Administrator user who is listing accounts. Optional.

Map configuration files protection

Determines whether other users can copy the map configuration files you have created for your account.

Status e-mail

Determines whether you receive a daily e-mail message about the status of the Peregrine appliance. If you set it to "Yes", you must also supply an e-mail address in *Account Contact Data* on page 287.

Append IP address

Determines whether or not device title hyperlinks also display the IP address for the device. Only affects devices for which an IP address is available. If the device title is already the IP address, the IP address will not be appended.

URL visibility

Determines whether or not device model and manufacturer hyperlinks also display the URL for the link. The visible URL can be cut and pasted, which can be handy for secure networks where external links are blocked.

Visible borders for text tables

When using the **Text** button to convert a table to an ASCII representation, determines whether or not to draw a border. Tables with a border are easier to interpret. Tables without a border are easier to cut and paste.

Color alternate table rows

Determines whether or not to color alternate rows in a table as light yellow. In large tables, alternating rows can make it easier to find data in the table.

Highlight table rows

Determines whether or not to highlight a table row as light blue when you position the mouse pointer over the row.

Visible navigation bar

Determines whether or not to include the Navigation Bar at the bottom of the screen—see *Navigation Bar* on page 44.

Time before marking statistic as stale

Determines how long before data in a table in the Device Manager, Port Manager, or Line Manager is considered stale and displayed with a gray background. (Data in the Device Manager Ports panel may be shown in parentheses instead of with a gray background.)

Long date format

Determines the format in which the date is reported:

- in Manager panels
- on Status pages

- on Report pages (generation date)
- in the Service Analyzer, Device Manager, Port Manager, and Line Manager (for example, to report how long a device has been broken)

Does not affect the date format used in the status bar of a map windows.

Use the date format codes shown in Table 2 to construct long dates and short dates.

Table 2: Date format codes

Code	Represents	Example
	Full Date	
%D	Date, numeric, American format (MM/DD/YY)	01/29/02
	Century	
%C	Century as 2-digit integer (year/100)	20
	Year	
%G	Year, ISO 8601, 4-digit. Same as Y%, unless the ISO week number (%V) belongs to the previous or next year, in which the previous or next year is used instead.	2002
%g	Year, ISO 8601, 2-digit.	02
%y	Year (abbreviated) (YY)	02
%Y	Year (YYYY)	2002
	Month	
%b	Month (abbreviated)	Jan
%B	Month	January
%h	Month (abbreviated). Equivalent to %b.	Jan
%m	Month (01-12)	01
	Week	
%a	Weekday (abbreviated)	Tue
%A	Weekday	Tuesday
%u	Weekday, numeric (1-7) Monday = 1	2
%w	Weekday, numeric (0-6) Monday = 0	1
%U	Week of the year (00-53). The first Sunday is the first day of week 01.	04
%V	Week of the year (01-53). Week 01 is the first week that has at least 4 days in the current year. Monday is the first day of the week.	05
%W	Week of the year (00-53). The first Monday is the first day of week 01.	04
	Day	
%d	Day of month (with leading zeroes)	29
%e	Day of month	29
%j	Day of year (001-366)	029
	Time	

Table 2: Date format codes (Continued)

Code	Represents	Example
%r	Time including AM/PM (HH:MM:SS xM)	02:43:08 PM
%R	Time, 24-hour clock (HH:MM)	14:43
%T	Time, 24-hour clock (HH:MM:SS)	14:43:08
%z	Time zone offset relative to UTC (or GMT)	-0500
%Z	Time zone (abbreviated)	EST
%p	"PM" or "AM"	PM
%P	"pm" or "am"	pm
	Hour	
%H	Hour, 24-hour clock, leading zeroes (00-23)	14
%I	Hour, 12-hour clock, leading zeroes (01-12)	02
%k	Hour, 24-hour clock, leading blanks (0-23)	14
%l	Hour, 12-hour clock, leading blanks (1-12)	2
	Minute and second	
%M	Minute (00-59)	43
%S	Seconds (00-61)	08
%s	Seconds since 1970-01-01 00:00:00 UTC (or GMT)	1012333388
	Special characters	
%n	Character: newline (or carriage return)	n/a
%t	Character: tab	n/a
%%	Character: percent	%

Short date format

Determines the format in which the date is reported at the bottom of the Manager Statistics panels' Table view, in Health Panel reports, in Reports tables, and in Status tables. Use the date format codes shown in Table 2 to construct long dates and short dates.

Help format

Determines the level of help associated with the Administration and Status pages and menus. Once you have gained experience with Network Discovery, you may wish to abbreviate the help shown. When help format is set to short, a Full Help link will appear. Click the Full Help link to have the complete help appear in a separate window called the Assistant.

Default Device Manager panel

Determines which panel is displayed when you open the Device Manager.

Default Port Manager panel

Determines which panel is displayed when you open the Port Manager.

Default Find panel

Determines which panel is displayed when you open the Find dialog.

Default Attribute Manager panel

Determines which panel is displayed when you open the Attribute Manager.

Default Device Manager Ports panel selection

Determines the default preference displayed when you open the Device Manager's Ports panel. Possible preferences are drawn from *Device Manager Ports Display Preferences* on page 376. Also determines how many rows are in the Ports panel's table.

Default Events Browser selection

Determines the default event selection displayed when you open the Events Browser, or when you open the Events panel in the Device Manager or in the Port Manager.

Procedural alerts

- You cannot change your account type or login status. Only an Administrator account can do this.
- If you leave the name blank, Network Discovery will make the name the same as the account login name.
- If you enter a blank date format, the default will be used.

Account Password

Changes the password used to access your Network Discovery account.

Passwords are case sensitive. "Magic", "magic", and "MAGIC" are three different passwords.

If you forget your password, the Network Discovery Administrator can create a new password for you.

Effects

You will have to log in again.

Limits

- *valid characters:* A–Z, a–z, 0–9, - *(hyphen)*, . *(period)*, _ *(underscore)*, @ *(at sign)*
- *length of input:* 4–20 characters

Procedural alerts

- You must enter your password twice to guard against typing errors.
- Do not enter your current password anywhere on this page.

Account Contact Data

Network Discovery monitors the events in your network. When an event occurs, Network Discovery can communicate with you via e-mail and via your pager once it knows how to contact you.

Table 3: Account Contact data

Contact via	Pager type	Information needed	Example
E-mail	—	user e-mail address	user@example.com
Pager	through e-mail gateway	pager gateway e-mail address	pager_gateway@provider.com
	direct to alphanumeric pager	■ pager number ■ pager service provider	■ 9-555-0903 ■ Bell Mobility; Cantel

Note: Network Discovery supports only alphanumeric pagers, not numeric pagers.

Limits

E-mail address and pager e-mail address

- *valid characters:* A–Z, a–z, 0–9, - *(hyphen)*, _ *(underscore)*, @ *(at sign)*, . *(period)*
- *length of input:* 0–60 characters

Pager number

- *valid characters:* 0–9
- *length of input:* 0–50 characters

Procedural alerts

- The list of pager service providers must be created by the Network Discovery Administrator. See *Pager Service Provider Configuration* on page 329.
- If the e-mail address is blank, you will not receive the status report, even when the receive list box is set to “yes”.
- You will normally select either direct or e-mail pager notification, and fill in the data only for one of these two options.

Test E-mail Address

Sends a test e-mail message to the e-mail address provided in *Account Contact Data* on page 287.

If you do not receive the message, it could be because:

- no e-mail address is provided
- an incorrect e-mail address is provided
- a mail server has not been specified for use with Network Discovery
- a server administrator e-mail address has not been specified for use with Network Discovery
- the Network Discovery mail server is not working
- the receiving mail server is not working

Test Pager Address

Sends a test message to your pager, using the information provided in *Account Contact Data* on page 287.

If you do not receive the page, it could be because:

- incorrect pager data is provided in the pager service provider profile
- no pager data is provided in your account profile
- incorrect pager data is provided in your account profile
- no external modem is connected to the Peregrine appliance
- the external modem connected to the Peregrine appliance is turned off
- there are modem synchronization problems
- there is no dial tone on the phone line being used
- your service provider is having problems
- your pager is turned off

Test Pager Number

Tests the pager number and profile of the pager service provider associated with your account.

You must have selected a service provider and entered a pager ID number for your account.

Requires a pager and pager number associated with the service provider.

If an error occurs and you do not receive the page, it could be because:

- incorrect pager data is provided in the pager service provider profile
- no pager data is provided in your account contact data
- no service provider profile is specified in your account contact data
- incorrect pager data is provided in your account contact date
- no external modem is connected to the Peregrine appliance
- the external modem connected to the Peregrine appliance is turned off
- there are modem synchronization problems
- there is no dial tone on the phone line being used
- your service provider is having problems
- your pager is turned off

Limits

- *valid characters:* 0–9
- *length of input:* 1-7 characters

Related

Although this option includes a test of the pager service provider, the provider itself will already have been tested by the Network Discovery Administrator with *Test Service Provider* on page 333.

My Map Configurations

Manage Map Configurations

Enables you to work with your own map configurations.

Options

- *copy:* duplicate your own map configurations
- *delete:* remove map configurations you no longer want
- *rename:* change the name of an existing map configuration
- *make current:* select the map configuration you want to have loaded the next time you open a map

Limits

You must not be using a map session.

Table 4: Map configuration name limits

Characteristic	Limits
Valid characters	A–Z, a–z, 0–9, - *(hyphen)*, _ *(underscore)**
Length of input	1–30 characters

* You may not put underscore characters at the beginning of the name.

Related

To copy map configurations belonging to other accounts, see *Copy Map Configurations* on page 290.

Copy Map Configurations

Enables you to copy map configurations from other accounts.

You may not copy your own map configurations with this option. To copy your own configurations for your own use, see *Manage Map Configurations* on page 290.

You may not copy your own map configurations *to* another account. Instead, the other account must use this option to request the map configurations *from* you.

When to use it

When another account has set up a template with custom packaging, icons, or titles.

Options

- You may specify a new name for the map configuration.
- You may use the existing name.

Limits

- You must not be using a map session.
- The account that owns the configurations must not be using a map session.
- The account that owns the configurations must have decided to allow other accounts to copy the configurations.
- The account that owns the configurations must have created at least one configuration.

Related

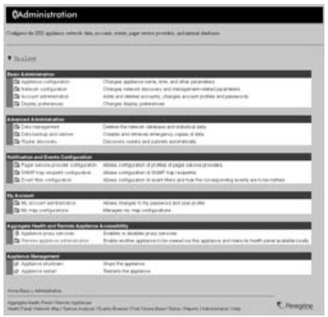
To copy your own configurations for your own use, see *Manage Map Configurations* on page 290.

20 CHAPTER Administration for Administrator Accounts

Figure 20-1: The two different Administration menus

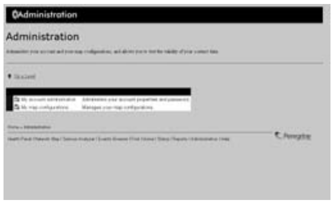
If your menu looks like this:

- Consult this chapter.



If your menu looks like this:

- See *Chapter 19, Administration for IT Employee and IT Manager Accounts*.



- Basic Administration
  - *Appliance Management* on page 293
  - *Account Administration* on page 306
  - *Network Configuration* on page 317
  - *Backup and Restore* on page 317
  - *Remote Appliance Administration* on page 327
- Notification and Events Configuration
  - *Pager Service Provider Configuration* on page 329
  - *SNMP Trap Recipient Configuration* on page 334
  - *Event Filter Configuration* on page 337
- Advanced Administration
  - *Network Tuning* on page 343
  - *Appliance Services* on page 356
  - *Data Management* on page 360
  - *Router Discovery* on page 365
  - *Display Preferences* on page 368
  - *Device Manager Ports Display Preferences* on page 376

- *My Account Administration* on page 379 see Chapter *19*, *Administration for IT Employee and IT Manager Accounts* —*My Account Administration* on page 282
- *My Map Configurations* on page 379 see Chapter *19*, *Administration for IT Employee and IT Manager Accounts* —*My Map Configurations* on page 290.

Introduction

Your account type determines the effect that the Administration button has.

IT Employee and IT Manager: To configure your own account, see *Chapter 19, Administration for IT Employee and IT Manager Accounts*.

Demo: You cannot perform any administration.

Administrator: You can create, delete and configure all types of accounts. You can also configure the Peregrine appliance and network operations.

Important: There can be more than one Administrator account. Two or more Administrator accounts can access Network Discovery simultaneously. In this situation, there is a risk of one Administrator account overwriting the work of another Administrator account. it is recommended that there be one Network Discovery Administrator.

- To shut down or restart the Peregrine appliance, see *Appliance Shutdown* on page 304 or *Appliance Restart* on page 305.
- To configure your Peregrine appliance for the *first* time, see the *Setup Guide*.
- To fine-tune the collection of data from your network, see the *Setup Guide*.
- To upgrade the Peregrine appliance for more capacity, see the *Setup Guide*.
- To create accounts for users, see *Add an Account* on page 308.
- To configure your own account, see *Chapter 19, Administration for IT Employee and IT Manager Accounts*.

Basic Administration

Basic administration includes:

- *Appliance Management* on page 293
- *Account Administration* on page 306
- *Network Configuration* on page 317
- *Backup and Restore* on page 317

Appliance Management

Appliance Management options are:

- *Appliance System Variables* on page 294
- *Appliance Community Strings* on page 295
- *Time Zone* on page 296
- *Domain Name Servers* on page 297
- *Host Name* on page 298
- *Workgroup* on page 299
- *Appliance Administrator E-mail Address* on page 299
- *SMTP Server* on page 300
- *NTP Server* on page 300
- *Generate licensing request* on page 301
- *Set Time* on page 302
- *Synchronize Time* on page 303
- *Appliance Shutdown* on page 304
- *Appliance Restart* on page 305

Here is where you manage your Peregrine appliance and the servers it uses to interact with your network.

Table 1: Appliance Management default settings

Feature	Setting	Default	Maximum
Appliance System Variables	System name	Unnamed	200 characters
	System contact	Unknown	200 characters
	System location	Unspecified	200 characters
Appliance Community Strings	Read-only	public	128 characters
	Read/write	private	128 characters
Time Zone		Canada/Eastern	—
Domain Name Servers	Servers	—	67 characters (10 servers)
	Search order	—	256 characters
Host Name		—	256 characters
Workgroup		WORKGROUP	15 characters
Appliance Administrator E-mail Address		—	60 characters
SMTP Server		—	256 characters
NTP Server		—	256 characters

In addition to the settings, there are also these actions:

- Generate Licensing Request
- Set Time

- Synchronize Time
- Appliance Shutdown
- Appliance Restart

Related *Appliance Services* on page 356

Appliance System Variables

System variables help to identify characteristics of the Peregrine appliance. The variables are system name, system contact, and system location.

Effects All information entered on this page also appears in the SNMP MIB of the Peregrine appliance. All users can view this information using the MIB Browser and the Configuration panel of the Device Manager. Object titles can also be set to any one of the three system variables—see *Device Title Preference* on page 369.

The system name appears in the banners of web browser windows, map windows, Manager windows, and the Health Panel. It is also used to identify the Aggregator appliance in the Aggregator Toolbar and in other places.

- The system contact is the person who should be contacted if there are problems with or questions about the Peregrine appliance.
- The system location is the physical location of the Peregrine appliance.

Limits

- *input:* 0–200 characters
- *time to change:* within 30 seconds

Default

- *system name:* Unnamed
- *system contact:* Unknown
- *system location:* Unspecified

Note: All the default values will be invisible to Network Discovery if left unchanged. See *Device Title Preference* on page 369. Also see **Help** > **Device Title Filters**.

Related

- To enter the e-mail address of the System Contact, *Appliance Administrator E-mail Address* on page 299.
- To make system variables capable of being clicked on (from within the Device Manager), see *Special input syntax* on page 36.

Appliance Community Strings

Community strings are a kind of password associated with a network device. These community strings control access to the SNMP MIB of the Peregrine appliance:

- The read-only community string controls read access to the Peregrine appliance's MIB.
- The read/write community string controls read and write access to the Peregrine appliance's MIB.

Note: Community strings are case-sensitive. "Public" and "public" are two different strings.

When to use it

We recommend that you:

- change the Peregrine appliance's read-only string to the one used by the rest of the devices in your network. The read-only community string allows read access to the Peregrine appliance MIB.
- change the Peregrine appliance's read/write community string (for security reasons). The read/write community string allows read and write access to the Peregrine appliance MIB

Effects

- These community strings affect only the Peregrine appliance itself.
- When you change one or both community strings, both are automatically recognized by Network Discovery and do not need to be included in the list of community strings (**Administration** > **Network Configuration** > **Community Property Groups**.)

Limits

- *input:* 0–128 characters
- *time to change:* within 30 seconds

Default

- *read-only:* public
- *read/write:* private

Related

To change the complete list of community strings within your entire network as managed by Network Discovery, see **Administration** > **Network Configuration** > **Community Property Groups**.

Time Zone

Network Discovery needs to know the time zone for the location of the Peregrine appliance so that Network Discovery can automatically calculate daylight savings time where appropriate. Local time is adjusted relative to Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT).]

Important: You must change the time zone the first time you use Network Discovery. If you wait, then change to a time zone earlier than the default, parts of Network Discovery will appear to halt. The Network Map will not be updated for a period equal to the difference between the default time zone and your time zone.

Effects

Sets the Peregrine appliance's clock.

Default

Canada/Eastern

Related

- To set the time, see *Set Time* on page 302.
- To synchronize the time once, see *Synchronize Time* on page 303.
- To synchronize the time repeatedly, see *NTP Server* on page 300.

Domain Name Servers

A domain name server translates between alphabetic domain names (also known as DNS names), such as "website.example.com", and numeric IP addresses, such as "192.168.96.1"—and vice versa. Network Discovery needs to know where your domain name servers are so that it can take advantage of this translation service.

Network Discovery also permits you to specify the order in which domains are searched (for the purposes of using abbreviated names with Find).

When to use it

Servers

- If you want domain names to appear on your Network Map, in your reports, when using Managers, and so on.

Note: If you leave the list of servers blank, devices will normally be referred to by IP address or MAC address throughout Network Discovery. You must enter at least one name server if you want to see domain names.

- If your network does not use any domain name servers, you may leave this item blank.

Search order

- If you want to save keystrokes when typing domain names.
- If you leave the search order list blank, it means that you will have to type the complete domain name for a device.

Effects

Search order

The domains you enter are used to extend domain names whenever you type them, and the order in which those extensions are applied to domain names. For instance, you might create a search order of "example.com,support.example.com, marketing.example.com". If you enter the name "eastern", Network Discovery would first try to match a device named "eastern.example.com", then one named "eastern.support.example.com", and finally "eastern.marketing.example.com".

Network Discovery stops as soon as it matches a domain name. Only an unsuccessful search causes Network Discovery to continue to the next item in the search order list.

Limits

Servers

- must be a valid IPv4 address
- *maximum servers:* 10
- *valid characters:* 0–9, . *(period)*
- *length of input:* 0–67 characters

Search order

- must be a valid domain name
- *valid characters:* A–Z, a–z, 0–9, - *(hyphen)*, . *(period)*
- *length of input:* 0–256 characters

Procedural alerts

Important: Network Discovery automatically restarts several processes after changing the domain name servers. Network Discovery does not respond for a short period after you click **Change**. This is normal.

Separate input with commas, spaces, or semi-colons.

Related To understand the effect that domain order has, see *Chapter 17, Find*.

Host Name

A host name allows you to refer to a device by a name rather than an IP address (much like a domain name). Network Discovery uses the host name to refer to itself in e-mails it sends.

The Host name page has two modes, prompted and manual.

Prompted mode

In prompted mode, Network Discovery tries to read its own host name from the domain name server. If Network Discovery finds a host name matching its IP address, you will be asked to confirm that the match is correct.

Note: You must have defined a domain name server first.

You are also given the opportunity to enter the host name yourself, as in manual mode.

Manual mode

In manual mode, Network Discovery has failed to find a match for its own IP address. You will be given the option to enter a host name.

Important: This is an advanced option. If you do not know what to enter, leave the field blank.

Limits

- *valid characters:* A–Z, a–z, 0–9, - *(hyphen)*, . *(period)*
- *length of input:* 5–256 characters

Default <*Peregrine appliance-IP-address*>.localdomain (e.g.: 192-168-5-2.localdomain)

Related To define a name server, see *Domain Name Servers* on page 297.

Workgroup

This option enables you to change the NetBIOS workgroup name. Workgroups are used primarily by Microsoft Windows.

The workgroup name determines where in your Network Neighborhood you find the shared NetBIOS folder of the Peregrine appliance.

The Peregrine appliance has a shared NetBIOS folder which you can use to deposit and retrieve:

- scan files
- updated software components you obtain from the Peregrine Support web site

Limits

- *valid characters:* A–Z, a–z, 0–9, - *(hyphen)*, . *(period)*
- *length of input:* 1–15 characters

Default

WORKGROUP

Procedural alert

Spaces are not permitted in the workgroup name.

Appliance Administrator E-mail Address

The Peregrine appliance requires an e-mail address to which it reports problems with the delivery of e-mail. Enter the e-mail address of the Network Discovery Administrator. This should be the same person listed for System Contact in *Appliance System Variables* on page 294.

If you tell Network Discovery about your *SMTP Server* on page 300, you must enter an e-mail address here.

Important: If you do not supply an e-mail address, no mail will be sent, even if Network Discovery has been configured with the address of your SMTP server.

If you enter an e-mail address that is not valid, you will cause “message undeliverable” e-mails to be sent to the account of the administrator for your network’s mail server (usually “postmaster”).

Limits

- must contain @ *(at sign)* and . *(period)*
- *valid characters:* A–Z, a–z, 0–9, - *(hyphen)*, . *(period)*, _ *(underscore)*, @ *(at sign)*
- *length of input:* 5–60 characters

Related

To have the same e-mail address capable of being clicked on (from the Device Manager), see System Contact in *Appliance System Variables* on page 294.

SMTP Server

An SMTP server is an electronic mail server that uses the Simple Mail Transport Protocol. Network Discovery uses a mail server to generate e-mail to notify you:

- (by default) whenever a device of priority 6 experiences an alarm, warning, or returns to normal—for details see *Event Filter Configuration* on page 337
- daily, about the health of your Peregrine appliance

The SMTP server can be part of your own network or outside your network.

Tip: If the SMTP server is outside your network, check that it will relay the mail from your appliance correctly.

If you specify an SMTP server, Network Discovery will relay all e-mail to the SMTP sever specified. If you do not specify an SMTP server, all e-mail will be sent in the normal SMTP way: directly from the Peregrine appliance to the mail server for the domain. This means that port 23 needs to be enabled on any intervening firewalls.

Limits

- *valid characters:* A–Z, a–z, 0–9, - *(hyphen)*, . *(period)*
- *length of input:* 0–256 characters

Procedural alerts

To enter the domain name of the mail server, you must have defined a domain name server first. You can always enter the IPv4 address of the mail server.

Related

Important: To complete the set-up of the mail server, see *Appliance Administrator E-mail Address* on page 299. If you do not supply this e-mail address, no mail will be sent.

NTP Server

An NTP server is a timekeeper server that uses the Network Time Protocol. The NTP server can be part of your own network or outside your network. Network Discovery uses the NTP server to synchronize the time continually—once every 120 minutes.

You only need to do one of these tasks:

- synchronize the time repeatedly (with an NTP server)
- synchronize the time once
- set the time

You do not need to do all three. However, you always need to set the time zone, whichever one of these you choose.

Limits

- *valid characters:* A–Z, a–z, 0–9, - *(hyphen)*, . *(period)*
- *length of input:* 0–256 characters

Technical

Time server compliant with RFC 1305

Procedural alerts

To enter the domain name of the time server, you must have defined a domain name server first. Otherwise, enter the IPv4 address of the time server.

Related

- To set the time zone, see *Time Zone* on page 296.
- To synchronize the time once, see *Synchronize Time* on page 303.

Generate licensing request

Enables you to request a license through the Network Discovery interface. The license can be for increased Network Discovery capacity or for a period of support from Peregrine Systems Customer Support

When to use it

Always used during setup. Network Discovery comes with a default license. The license gives you:

- capacity for one map session at a time
- the ability to find ten devices on the network
- the ability to have ten resource-managed devices

You can use Network Discovery with the default license temporarily until you request and receive the license that gives you the full functionality you purchased.

Use it when you need to increase Network Discovery's capacity, for instance, because you now have more devices than your original license covers or because you now need a license for an Aggregator or because you need to extend your support contract.

Always make sure your maintenance license is up to date before you update your Network Discovery software or download software components.

Effects

Peregrine Systems Customer Support generates your new license file and sends it to you attached to an e-mail.You must install the license after you receive it. For instructions, see the *Setup Guide*.

If the license is not appropriate, Network Discovery does not perform the installation and moves the file to the shared directory, \\<appliance IP>\share\license\bad.

If the license asks the Peregrine appliance to do too much, (for example, a license for more devices than the Peregrine appliance can support) the Peregrine appliance will take the maximum it can do.

Options

If your Peregrine appliance is configured to send e-mail (*Appliance Administrator E-mail Address* on page 299), you can either send your request directly from the appliance or you can cut and paste the information into an e-mail.

If your Peregrine appliance is not configured to send e-mail, enter the information requested on the form into an e-mail and send it to support @peregrine.com.

Procedural alerts

If you purchased Network Discovery from an Original Equipment Manufacturer or a Value-Added Reseller, follow your OEM/VAR's instructions to obtain a license.

Related commands

To see what licenses are currently installed on your Peregrine appliance, see **Status** > **Current Settings** > **Installed Licenses**.

You can also compare your software components (**Status** > **Current settings** > **Installed components**) to the latest at support.peregrine.com and download any new ones. For instructions, see the *Setup Guide*.

Set Time

The date and time are used by Network Discovery for scheduling actions such as updating and generating reports, and for date-stamping mail, reports, pages, and Manager panels.

You only need to do one of these tasks:

- set the time
- synchronize the time once
- synchronize the time repeatedly (with an NTP server)

You do not need to do all three. However, you always need to set the time zone, whichever one of these you choose.

Effects

The Peregrine appliance's clock is updated. Seconds are set to zero.

Limits

- *year:* 1970–2037
- *day:* 1–31
- *hour:* 0–23
- *minute:* 0–59

Procedural alerts

Before you begin, make sure the time zone is set correctly.

Warning: Do not change the date and time significantly once the date, time, and time zone have been set. You will erase your Network Map or freeze your Network Map.

If you set the date and time forward, Network Discovery examines the "last seen" date for all devices on your map and removes all the devices it hasn't seen. If the difference is greater than the periods specified by Device Purge Intervals in *Expiry* on page 352, Network Discovery purges all devices from your Network Map.

If you set the date and time back (or set them forward and then back), Network Discovery will appear to halt. The Network Map will not be updated for a period equal to the difference between the current time and the latest time it has ever seen. For example, if you accidentally type the year as "2004" when you meant 2003 and later have to set the year, correctly, to 2003, then Network Discovery will take one year to start updating the map again. This problem can only be rectified with the help of Peregrine Systems Customer Support.

Related

- To set the time zone, see *Time Zone* on page 296.
- To synchronize the time once, see *Synchronize Time* on page 303.
- To synchronize the time repeatedly, see *NTP Server* on page 300.

Synchronize Time

Network Discovery uses an NTP server to synchronize *continually*. The NTP server can be part of your own network or outside your network. An NTP server is a timekeeper server that uses the Network Time Protocol.

You only need to do one of these tasks:

- synchronize the time once
- synchronize the time repeatedly (with an NTP server)
- set the time

You do not need to do all three. However, you always need to set the time zone, whichever one of these you choose.

Limits

- *valid characters:* A–Z, a–z, 0–9, - *(hyphen)*, . *(period)*
- *length of input:* 0–256 characters

Default

- *initial:* blank
- *subsequent:* time server name as specified in *NTP Server* on page 300, unless blank

Technical

Time server compliant with RFC 1305

Procedural alerts

Before you begin, make sure the time zone is set correctly.

Warning: Do not change the date and time significantly once the date, time, and time zone have been set. You will erase your Network Map or freeze your Network Map.

If you set the date and time forward, Network Discovery will examine the "last seen" date for all devices on your map and remove all the devices it hasn't seen. If the difference is greater than the periods specified by Device Purge Intervals in *Expiry* on page 352, Network Discovery will purge all devices from your Network Map.

If you set the date and time back (or set them forward and then back), Network Discovery will appear to halt. The Network Map will not be updated for a period equal to the difference between the current time and the latest time it has ever seen. For example, if you accidentally type the year as "2004" when you meant 2003 and later have to set the year, correctly, to 2003, then Network Discovery will take one year to start updating the map again. This problem can only be rectified with the help of Peregrine Systems Customer Support.

Related

- To set the time zone, see *Time Zone* on page 296.
- To synchronize the time once, see *Synchronize Time* on page 303.
- To set the time, see *Set Time* on page 302.

Appliance Shutdown

Shuts down the Peregrine appliance.

Warning: It is extremely important to shut down the Peregrine appliance properly. If the correct procedure is not followed, you risk corrupting the data on the Peregrine appliance. Make sure that every person who may come into contact with the Peregrine appliance understands how to shut the Peregrine appliance down properly.

Tip: Be sure to include the people who clean and make repairs in the room where you keep your Peregrine appliance.

The Peregrine appliance is designed to restart and recover from power interruptions automatically. However, interrupting the hard drive when it is writing data can corrupt data on the hard drive. Whenever possible, the Peregrine appliance should be powered off in an orderly fashion. For this reason, we strongly recommended the use of a UPS with Network Discovery.

Note: You can also shut down the Peregrine appliance through the configuration interface.

When to use it

- When performing scheduled maintenance.
- When physically moving the Peregrine appliance.
- In advance of a scheduled power outage.

Effects

Resets the Peregrine appliance uptime.

Procedural alerts

Warning: Do not shut off the appliance if there is disk activity. You can damage the Peregrine appliance's hard drive

After you click **Shut down appliance**, wait until the screen shows "The system is halted" before you before you power off the Peregrine appliance.

Related

To shut down the Peregrine appliance using the configuration interface, see the *Setup Guide*, "Shutting Down the Peregrine Appliance".

Appliance Restart

Restarts the Peregrine appliance.

Note: You can also restart the Peregrine appliance through the configuration interface.

When to use it

You have been advised to do so on the Activate Changes page.

Effects

- checks the Network Discovery database
- disconnects all map sessions
- restarts the Peregrine appliance uptime
- attempts to verify the host name (if unsuccessful, deletes host name data)

Procedural alerts

- Wait at least 10 minutes after clicking **Restart appliance**.
- You will not see any indication of the progress or successful completion of the restart. We recommend that you use the configuration interface with a keyboard and monitor connected directly to the Peregrine appliance, which does give such indication.

Related

To restart the Peregrine appliance through the configuration interface, see the *Setup Guide*, “Restarting the Peregrine Appliance”.

Account Administration

These are the account features:

- *List Accounts* on page 307
- *Add an Account* on page 308
- *Account Properties* on page 309
- *Account Contact Data* on page 315
- *Account Password* on page 316
- *Delete an Account* on page 316

Each Network Discovery user must have an account. The types of account and their privileges are discussed in *Chapter 2, Terms and Concepts*, in the section *Account types* on page 31.

Important: There can be more than one Administrator account. If two or more Administrator accounts access Network Discovery simultaneously, there is a risk of one Administrator account overwriting the work of another Administrator account. It is recommended that there be only one Network Discovery Administrator.

IT Employee and IT Manager users can perform limited administration on their own accounts, but only the Network Discovery Administrator (or other Administrator account) can add, set up, and delete accounts. The Network Discovery Administrator must also do administration for Demo accounts, since Demo accounts have no access to administration.

List Accounts

Lists all accounts. The list is sorted alphabetically by login name.

The login names are hyperlinked. A hyperlink takes you to a shortcut menu for that account.

Default

When you receive it, Network Discovery has four default accounts:

Table 2: Default accounts

Account type	Account name	Password
Demo	demo	demo
IT Employee	itemployee	password
IT Manager	itmanager	password
Administrator	admin	password

To increase security, create a new "Administrator" account with different a login name and password, then delete the default accounts.

Important: If you delete the "Administrator" account, you must also change the default event filters, "email-admin-device" and "email-admin-line"—see *List Filters* on page 338.

Add an Account

Creates an account. An account and password permit a user to log in to Network Discovery.

Limits

- *total accounts:* 1–250
- *name—valid characters:* a–z, 0–9, _ *(underscore); first character cannot be underscore*
- *name—length of input:* 3–20 characters
- *reserved names:* adm | alias | bin | daemon | ftp | games | halt | loran | lp | mail | news | nobody | operator | peregrine | qmaild | qmaill | qmailp | qmailq | qmailr | qmails | root | shutdown | sync | uucp | www

Procedural alerts

- Any letters must be lower case (a–z).
- You must still create a password for the account. If you do not create a password, the account will not permit logins.
- If you create an account with the name “admin”, its account type will be Administrator. If you create an account with the name “demo”, its account type will be Demo. If you create an account with any other account name, its default account type will be IT Employee, but you can change its account type.

Related

- To modify the account type and other properties, see *Account Properties* on page 309.
- To create a password, see *Account Password* on page 316.

Account Properties

Customizes the display format and permissions for an account.

Options

Table 3: Account properties options

Option	Setting	Limits	Default
Account type		Administrator | IT Employee| IT Manager| Demo	IT Employee*
Account capabilities	Web Access	Yes | No	Yes
	MySQL ODBC Access	Yes | No	No
	ApE Access	No (no license)	No
	Shared directory Access	Yes | No	No
Name		■ *valid characters:* A–Z, a–z, 0–9, - *(hyphen)*, _ *(underscore)*, *(space)* ■ *length of input:* 0–40 characters	—
Allow others to copy map configurations?		Yes | No	No
Append IP address to device titles?		Yes | No	No
Make URLs visible?		Yes | No	No
Draw borders on tables in text mode?		Yes | No	No
Alternate colors in table rows?		Yes | No	Yes
Highlight table rows on mouse over?		Yes | No	No
Show navigation bar?		Yes | No	Yes
Time before marking statistic as stale		Days, Hours, Minutes, Seconds	2 hours
Long date format		See Table 21 on page 312	%A, %B %e, %Y %T %Z
Short date format		See Table 21 on page 312	%Y-%m-%d %R
Inline help format		All | Short	All
Default Device Manager panel		Configuration | State | Statistics | Ports | Events | IP Ping | Traceroute | SNMP Ping | DNS Query | Update Model [Administrator only] | Diagnosis	State
Default Port Manager panel		Configuration | State | Diagnosis | Statistics | Events	State
Default Find panel		Device | Port | Advanced	Device
Default Attribute Manager panel		Configuration | Statistics	Configuration

Table 3: Account properties options (Continued)

<table>
<tr><th>Option</th><th>Setting</th><th>Limits</th><th>Default</th></tr>
<tr><td>Default Device Manager Ports panel selection</td><td>Selection</td><td>| Status | Details | see <em>Device Manager Ports Display Preferences</em> on page 376</td><td>Status</td></tr>
<tr><td></td><td>Increment</td><td>1–1000</td><td>24</td></tr>
<tr><td>Default Events Browser selection</td><td>Selection</td><td>All | Line Breaks | Utilization | Delay | Collisions | Broadcasts | Device Breaks | Packet Loss | Adds | Deletes</td><td>All</td></tr>
<tr><td></td><td>Increment</td><td>1–1000</td><td>20</td></tr>
</table>

* There are two exceptions: an account named “admin” will have an account type of Administrator, and an account named “demo” will have an account type of Demo.

Important: There can be more than one Administrator account. If two or more Administrator accounts access Network Discovery simultaneously, there is a risk of one Administrator account overwriting the work of another Administrator account. It is recommended that there be only one Network Discovery Administrator.

Only an Administrator account can change the account type and account capabilities. Also, you cannot change the account type or account capabilities of the account you are currently using.

Note: *for Aggregator*—You must check the account type carefully, since data retrieval for the Aggregate Health Panel requires not only an identical account name, but also the identical account type and *Account Password* on page 316.

Table 20-1: Account properties that Administrator accounts control

Property	Explanation
Account type	Determines the account’s level of access to Network Discovery.
Account capabilities:	Determines what capabilities of Network Discovery the account can access
■ Web Access	■ allows owner to use Network Discovery. You will probably enable this, but conceivably the user only needs MySQL ODBC access or access for scan files from Peregrine’s Inventory (the Windows Management Instrumentation (WMI) collector).
■ MySQL ODBC Access	■ allows owner of the account to export Network Discovery data to third-party data access applications to create custom reports. **Note:** You cannot set this option to “Yes”, if you have disabled Remote MySQL access in **Administration** > **Appliance Services** > **Remote MySQL access enabled** (*MySQL Access* on page 357).
■ Shared directory Access	■ the shared directory is for downloading license files and Express Inventory, the WMI collector scan files
Name	The name of the account owner.

Property	Explanation
Allow others to copy map configurations	Determines whether or not other users can copy map configuration files from this account.
Append IP Address to device titles?	Determines if device titles are followed by device IP addresses (when available).
Make URLs visible	Determines if hyperlinks are followed by the associated URL (for easy cut and paste).
Draw borders on tables in text mode	If you use the “as text” button, tables will have borders. Tables are easier to read with borders, but they take up more space on your screen.
Alternate colors in table rows	Tables are easier to read with alternating colors, but they take more space on your screen.
Highlight table rows on mouse over	Lets you highlight a row you want to look at.
Show navigation bar	Determines whether or not you see the navigation hyperlinks at the bottom of pages. The hyperlinks are the same as the buttons on the Toolbar.
Time before marking statistic as stale	Determines how long before data in a table in the Device Manager, Port Manager, or Line Manager is considered stale and displayed with a gray background. (Data in the Device Manager Ports panel may be shown in parentheses instead of with a gray background.)
Long date format	Determines how the date is displayed at the bottom of most panels and pages.
Short date format	Determines how the date is displayed at the bottom of the Statistics panel's Table view and in Reports, Event Browser and Health Panel.
Inline help format	Determines if you automatically see short or full help files in HTML menus. If you choose the short help option, you see a link called “Full Help”. Clicking that link opens an Assistant window that displays the Full Help.
Default Device Manager panel	Determines which panel appears initially when you open a Device Manager session.
Default Port Manager panel	Determines which panel you see first when you open a Port Manager session.
Default Find panel	Determines which panel you see first when you open a Find session.
Default Attribute panel	Determines which panel you see first when you open an Attribute Manager session.

Property	Explanation
Default Device Manager Ports panel selection - increment	Determines which panel you see first when you open a Ports session from the Device Manager. Possible preferences are drawn from *Device Manager Ports Display Preferences* on page 376. - Determines how many rows of data the Ports panel displays at a time. Default: 24
Default Events Browser selection - increment	Determines which panel you see first when you open an Events Browser session.You can see all of the events or choose one. - Determines how many rows of data the Events Browser displays at a time. Default: 20

Draw borders on tables in text mode

When using the **Text** button to convert a table to an ASCII representation, determines whether or not to draw a border. Tables with a border are easier to interpret, but they take up more space on the screen.

Long date format

Determines the format in which the date is reported:

- in Manager panels
- on Status pages
- on Report pages (generation date)
- in the Service Analyzer, Device Manager, Port Manager, and Line Manager (for example, to report how long a device has been broke)

Does not affect the date format used in the status bar of a map windows.

Use the date format codes shown in Table 21 on page 312 to construct long dates and short dates.

Table 21: Date format codes

Code	Represents	Example
	Full Date	
%D	Date, numeric, American format (MM/DD/YY)	01/29/02
	Century	
%C	Century as 2-digit integer (year/100)	20
	Year	
%G	Year, ISO 8601, 4-digit. Same as Y%, unless the ISO week number (%V) belongs to the previous or next year, in which the previous or next year is used instead.	2002
%g	Year, ISO 8601, 2-digit.	02
%y	Year (abbreviated) (YY)	02
%Y	Year (YYYY)	2002

Table 21: Date format codes (Continued)

Code	Represents	Example
	Month	
%b	Month (abbreviated)	Jan
%B	Month	January
%h	Month (abbreviated). Equivalent to %b.	Jan
%m	Month (01-12)	01
	Week	
%a	Weekday (abbreviated)	Tue
%A	Weekday	Tuesday
%u	Weekday, numeric (1-7) Monday = 1	2
%w	Weekday, numeric (0-6) Monday = 0	1
%U	Week of the year (00-53). The first Sunday is the first day of week 01.	04
%V	Week of the year (01-53). Week 01 is the first week that has at least 4 days in the current year. Monday is the first day of the week.	05
%W	Week of the year (00-53). The first Monday is the first day of week 01.	04
	Day	
%d	Day of month (with leading zeroes)	29
%e	Day of month	29
%j	Day of year (001-366)	029
	Time	
%r	Time including AM/PM (HH:MM:SS xM)	02:43:08 PM
%R	Time, 24-hour clock (HH:MM)	14:43
%T	Time, 24-hour clock (HH:MM:SS)	14:43:08
%z	Time zone offset relative to UTC (or GMT)	-0500
%Z	Time zone (abbreviated)	EST
%p	“PM” or “AM”	PM
%P	“pm” or “am”	pm
	Hour	
%H	Hour, 24-hour clock, leading zeroes (00-23)	14
%I	Hour, 12-hour clock, leading zeroes (01-12)	02
%k	Hour, 24-hour clock, leading blanks (0-23)	14
%l	Hour, 12-hour clock, leading blanks (1-12)	2
	Minute and second	
%M	Minute (00-59)	43
%S	Seconds (00-61)	08
%s	Seconds since 1970-01-01 00:00:00 UTC (or GMT)	1012333388

Table 21: Date format codes (Continued)

Code	Represents	Example
	Special characters	
%n	Character: newline (or carriage return)	n/a
%t	Character: tab	n/a
%%	Character: percent	%

Short date format

Determines the format in which the date is reported at the bottom of the Manager Statistics panels' Table view, in Health Panel reports, in Reports tables, and in Status tables. Use the date format codes shown in Table 21 on page 312 to construct long dates and short dates.

Inline help format

Determines the level of help associated with the Administration and Status pages and menus. Once you have gained experience with Network Discovery, you may wish to abbreviate the help shown. When help format is set to short, a Full Help link will appear. Click the Full Help link to have the complete help appear in a separate window called the Assistant.

Procedural alerts

- Except for account type and account capabilities, Account Properties can be modified by the owner of the account, as well as by Administrator users.
- If no password is given, the account cannot be used to log in, even when login status is set to "yes".
- You cannot change the account type or account capabilities for the account you are currently using.
- You cannot change the login status for the account you are currently using.
- If you leave the name blank, Network Discovery will make the name the same as the account login name.
- If you enter a blank date format, the default will be used.

Related

To ensure that the account is login enabled, enter an *Account Password* on page 316.

Account Contact Data

Because Network Discovery can alert you to events in your network, users must inform Network Discovery how they wish to be contacted, by e-mail or by alphanumeric pager.

Table 22: Account Contact data

Contact by	Pager type	Information needed	Example
E-mail	—	user e-mail address	user@example.com
Pager	through e-mail gateway	pager gateway e-mail address	pager_gateway@provider.com
	direct to alphanumeric pager	■ pager number ■ pager service provider	■ 9-555-0903 ■ Bell Mobility; Cantel

Note: Network Discovery supports only alphanumeric pagers, not numeric pagers.

The list of pager service providers must be created by the Network Discovery Administrator. See *Pager Service Provider Configuration* on page 329.

Effects

The e-mail address supplied here affects the default address for *External Backup Configuration* on page 318.

Limits

E-mail address and pager e-mail address:

- *valid characters:* A–Z, a–z, 0–9, - *(hyphen)*, _ *(underscore)*, @ *(at sign)*, . *(period)*
- *length of input:* 0–60 characters

Pager number

- *valid characters:* A–Z, a–z, 0–9, - *(hyphen)*, _ *(underscore)*, @ *(at sign)*, . *(period)*
- *length of input:* 0–50 characters

Procedural alerts

The user will normally select either direct or e-mail pager notification, and fill in the data only for one of these two options.

Related

- To create a list of pager service providers, see *Pager Service Provider Configuration* on page 329.
- To determine which events a user is interested in, see *Event Filter Configuration* on page 337.

Account Password

Creates or modifies the password associated with an account.

Passwords are case sensitive. “MAGIC”, “magic”, and “Magic” are three different passwords.

Important: If no password is given, the account cannot be used to log in, even when login status is set to “yes”.

Note: *for Aggregator*—Data retrieval for the Aggregate Health Panel requires not only an identical account name, but also an identical password.

Effects If you change your own password, you will have to log in again.

Limits

- *valid characters:* A–Z, a–z, 0–9, - *(hyphen)*, _ *(underscore)*, @ *(at sign)*, . *(period)*
- *length of input:* 4–20 characters

Procedural alerts

- Entering the same password twice helps guard against typing errors.
- Do not enter the current account password anywhere on this page.

Delete an Account

Deletes an account.

Effects The user will not be able to log in to the account unless you recreate the account with *Add an Account* on page 308.

Limits You cannot delete the account you are currently using.

Network Configuration

For information on Network Configuration, see the *Setup Guide*.

Backup and Restore

These are the backup options:

- *External Backup Configuration* on page 318
- *Run Internal Backup Now* on page 320
- *Run External Backup Now* on page 320
- *Restore from Internal Backup* on page 321
- *Restore from Tape* on page 321
- *Restore from FTP* on page 322
- *Restore from Another Appliance* on page 323
- *Check Backup File Size* on page 324
- *Test External Backup and Restore* on page 325
- *View Backup Log* on page 326
- *View Restore Log* on page 326
- *View Test Log* on page 326

You can back up data (a routine operation) and you can restore data (an emergency recovery). A backup can have these properties:

- scheduled or immediate
- internal or external

A restoration can have these properties:

- internal or external

(You cannot have a scheduled restore, because restoring data is not a routine operation.)

An internal backup copies the active data to a backup partition. An internal backup involves only the hard drive within the Peregrine appliance.

Note: Whenever an internal backup is done (scheduled or immediate), Network Discovery will also perform an external backup if configured.

The scheduled internal backup takes place every 24 hours, shortly after midnight. (An external backup will take place immediately afterward, if configured.)

An external backup copies the data from the backup partition to external storage media—either a tape drive or an FTP server, or both.

There are three places from which you restore externally:

- tape drive (if external backup was made)

- FTP server (if external backup was made)
- another Peregrine appliance

Note: Whenever an external restore is done (from FTP, tape, or another appliance), both the internal backup and the active data are overwritten. (This happens regardless of whether the internal backup has been backed up externally.)

External Backup Configuration

Controls whether Network Discovery creates a scheduled external backup of the Peregrine appliance's data on a USB tape drive, or as a file on a device that supports FTP. Also controls the parameters for immediate backups.

External backups are made approximately every 24 hours, some time after midnight, and after the internal backup. If the internal backup fails, the external backup will not proceed.

Note: External backups are not scheduled until the Peregrine appliance has been in use for at least 2 hours. For example, if you attach your Peregrine appliance to your network at an hour before midnight, or 2300 (11 PM), and request an external backup, the backup cannot begin until 0100 (1 AM).

Note: If a backup fails, Network Discovery generates an e-mail (assuming Network Discovery is configured to allow this). Network Discovery waits 30 minutes, then tries again to create a backup. Each failure generates a new e-mail.

When to use it

- If you do not have a USB tape drive connected to your Peregrine appliance, turn the daily tape backup to **Off**.
- If you do not have a backup file repository that supports FTP, turn the daily FTP backup to **Off**.

Table 23: External backup options

Option	Limits	Default
Tape *(active)*	On | Off	Off
FTP *(active)*	On | Off	Off
Username*†	■ *valid characters:* A–Z, a–z, 0–9, @ *(at sign)*,. *(period)*, - *(hyphen)* ■ *length of input:* 4–20 characters	—
Password*	4–60 characters	—
Host name or IPv4 address*	■ *valid characters:* A–Z, a–z, 0–9,. *(period)*, - *(hyphen)* ■ *length of input:* 1–50 characters	—
Directory	■ *valid characters: any, except* / *(slash) and* \ *(backslash)* ■ *length of input:* 0–256 characters	top-level directory associated with username
Filename	■ *valid characters: any* ■ *length of input:* 1–256 characters	<*yyyymmdd*>.tar
Port	1–65,535	21

Table 23: External backup options (Continued)

Option	Limits	Default
Back up scan files to FTP	Yes | No	No
Send e-mail on success *(active)*	Yes | No	No
Send e-mail on failure *(active)*	Yes | No	Yes
E-mail address	0–50 characters	—

* Required field.

† You should create a special account on the repository device with very few security privileges.

Peregrine has tested the following FTP servers:

- Windows 95 and Windows 98 running IIS
- Windows NT Server (IIS)
- Windows 2000 Professional (IIS 4)
- Red Hat Linux: Kernel 2.2.12, ProFTPD version 1.2.6

Note: Backups can get quite large, so make sure that the target platform can support files of 2 GigaBytes or more.

Procedural alerts

If you do not have a USB tape drive connected to your Peregrine appliance, ensure that the tape option is Off.

The default is Off.

Note: The tape option does not appear if you do not have a tape drive connected. However, the tape option *does* still appear, if you disconnect the tape drive after you have configured the external backup as “Tape On”.

Note: If you have just restored a backup from an older appliance that did have a tape drive installed, the tape option may appear even though you no longer have a tape drive installed.

- For FTP, it is your responsibility to ensure that the username, password, host name or IP address, directory, filename and port are all valid. For example, if you create a filename containing illegal characters, the backup will fail. You should *Test External Backup and Restore* on page 325, every time you make a change.
- For FTP, it is your responsibility to ensure that the username has read and write permission for the directory specified.
- *Optional:* You can insert special date characters in the filename. These are some of the same date characters as used in long and short date format in *Account Properties* on page 309.
- E-mail option will not be available if:
  - the SMTP server is not set up
  - the e-mail address is not provided
  - the account contact data does not include an e-mail address

Run Internal Backup Now

Causes the active data to be copied to an internal backup immediately, instead of waiting for the automatic daily internal backup.

Running an immediate internal backup never interferes with the automatic daily internal backup:

- The immediate backup does not prevent the automatic backup from happening.
- If an internal backup is already in process, this does not begin a second internal backup. Network Discovery informs you that the internal backup is running, and asks you to try later.

Note: Network Discovery does not respond for a short period after you click **Backup now**. This is normal.

Effects

- Also initiates an external backup, if one has been configured.
- Several items in the *Appliance Management* menu will not be available while the backup is running.

Related To cause an immediate external backup see *Run External Backup Now*, next.

Run External Backup Now

Causes the internal backup to be copied to the tape drive and/or sent by FTP to the external device. Asks for confirmation.

Uses parameters entered under *External Backup Configuration* on page 318.

Warning: If tape backup is selected, the tape in the drive will be erased.

If an internal backup is in process, the external backup will not begin. Network Discovery will inform you that the internal backup is running, and ask to try later.

Limits You cannot run an external backup that does not use an internal backup.

Does not cause the active data to be copied to the internal backup.

Example: If you run the external backup at 1700 (5 PM), you are only causing the internal backup, made the previous midnight, to be copied to the tape drive and/or by FTP. The work you have done between midnight and 1659 (4:59 PM) will not backed up until midnight, seven hours later.

Procedural alert If FTP is selected, it creates a temporary file—<*filename*>.ftp.test.file—then erases it.

Related To cause an immediate internal backup, see *Run Internal Backup Now*.

Restore from Internal Backup

Transfers the internal backup to the active data being used by Network Discovery.

Important: Overwrites the active data. This action cannot be undone.

Effects

Note: Network Discovery does not respond for a short period after you click **Restore**. This is normal.

Several items in the *Appliance Management* menu will not be available while the restore is running.

Restore from Tape

Transfers the tape backup to the internal backup partition on the Peregrine appliance, then transfers the internal backup to the active data being used by Network Discovery.

Confirms selection of tape.

Important: Overwrites the active data. This action cannot be undone.

Limits

Will only transfer backups created for the current version and versions that are data compatible. (For details, see the Release Notes in the Help menu.)

Restore from FTP

Transfers the files by FTP from the external device to the internal backup partition on the Peregrine appliance, then transfers the internal backup to the active data being used by Network Discovery.

Important: Overwrites the active data. This action cannot be undone.

Enables you to select a filename on the external device. Displays date of backup and version of Network Discovery used to create the backup.

Table 24: External backup options

Option	Limits	Default
Username*	■ *valid characters:* A–Z, a–z, 0–9, @ *(at sign)*, . *(period)*, - *(hyphen)* ■ *length of input:* 4–20 characters	—
Password*	4–60 characters	—
Host name or IPv4 address*	■ *valid characters:* A–Z, a–z, 0–9, . *(period)*, - *(hyphen)* ■ *length of input:* 1–50 characters	—
Directory	0–256 characters	—
Port	1–65,535	21
Send e-mail on success *(active)*	Yes | No	No
Send e-mail on failure *(active)*	Yes | No	Yes
E-mail address	0–50 characters	—

* Required field.

Limits Will only transfer backups created for the current version and version that are data compatible.

Procedural alert It is your responsibility to ensure that the username has read and write permission for the directory specified.

Restore from Another Appliance

Causes this Peregrine appliance to copy data from a second Peregrine appliance to this Peregrine appliance.

Important: Overwrites the active data. This action cannot be undone.

Use a cross over cable to connect the two appliances. Connect the cross over cable to Ethernet port 2 on the PND appliance (either the IBM xSeries 335 or the IBM xSeries 330).

Figure 20-2: Ethernet port 2 on the IBM xSeries 335

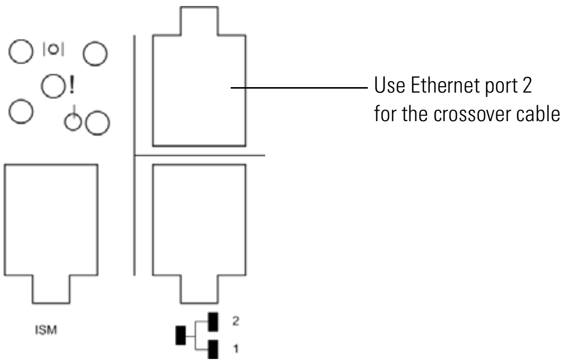
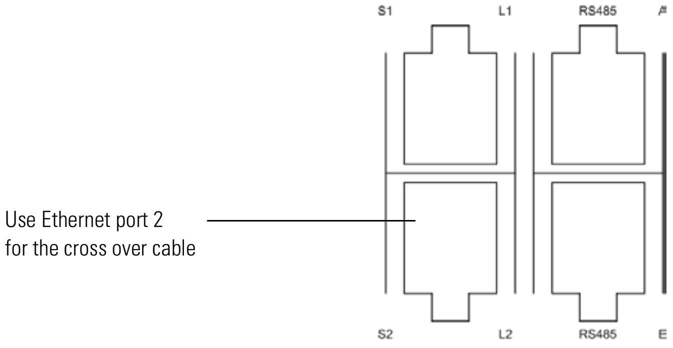


Figure 20-3: Ethernet port 2 on the IBM xSeries 330



When you click **Restore**, the copy is scheduled for one minute later. The data will be copied to this Peregrine appliance as a backup, then the backup replaces the active data for this appliance.

Note: Network Discovery does not respond for a short period after you click **Restore**. This is normal.

To confirm the success of the transfer, *View Restore Log* on page 326.

Note: The cross over connections are temporarily assigned the IP addresses of 209.167.240.70 and 209.167.240.71. The Peregrine appliance does not route using these addresses. These IP address assignments are removed after the data transfer.

When to use it

- When you need to copy data from an Peregrine appliance that you will be returning to Peregrine Systems for repair or replacement.
- To migrate data from one appliance to another in order to migrate from IND 4.2 or 4.3 or from (see the *Setup Guide* for more detail).

An IND 4.2 or 4.3 appliance will detect the absence of a cable in its own cross over connection, but cannot detect whether the correct cable is being used, or whether the far end of the cable is connected correctly.

Note: Xanadu does not support the cross over cable.

Important: You must attach the cross over cable between the two associated connections. The cable also fits in the network connection, but this method of connecting will result in no transfer.

Limits

Both appliances must have installed IND version 4.2 or 4.3, or Network Discovery 5.0.x.

Procedural Alert

Network Discovery does not give you a request for confirmation. When you click Restore, Network Discovery begins the Restore process.

Check Backup File Size

Reports the disk space required by the backup (in megabytes).

When to use it

- To determine whether you have sufficient space on your FTP server for the backup.

Test External Backup and Restore

Allows test of *External Backup Configuration* on page 318.

For tape backup/restore, Network Discovery checks:

- whether a tape drive can be found
- whether a tape is in the drive

Warning: If tape is selected, the tape in the drive will be erased.

For FTP backup/restore, Network Discovery checks:

- the existence of the device specified
- whether the username and password work for the device
- the port specified for the device
- read/write ability for the device

If a directory is specified, Network Discovery checks whether the directory exists and whether the directory can be written to.

For appliance restore, Network Discovery checks:

- the connection to the second Peregrine appliance
- that the second Peregrine appliance can provide data
- that the data on the second Peregrine appliance is compatible with the active appliance

Procedural alerts

- If no filename has been specified, Network Discovery will use for the name the number of seconds since 1970-01-01 00:00:00 UTC.
- If FTP is selected, it will create a temporary file—<*filename*>.ftp.test.file—then erase it.

View Backup Log

Displays the details of external backups. All available logs for the past 30 days are shown, in reverse chronological order (most recent log first). The name of the log is always the exact date and time at which the backup was started.

Note: The backup logs themselves are neither backed up nor restored.

Related To perform a backup, see:

- *Run Internal Backup Now* on page 320
- *Run External Backup Now* on page 320

View Restore Log

Displays the details of restorations. All available logs for the past 30 days are shown, in reverse chronological order (most recent log first). The name of the log is always the exact date and time at which the restoration was started.

Note: The restore logs themselves are neither backed up nor restored.

Related To restore data, see:

- *Restore from Internal Backup* on page 321
- *Restore from Tape* on page 321
- *Restore from FTP* on page 322
- *Restore from Another Appliance* on page 323

View Test Log

Displays the details of test. All available logs for the past 30 days are shown, in reverse chronological order (most recent log first). The name of the log is always the exact date and time at which the restoration was started.

Note: The test logs themselves are neither backed up nor restored.

Related To perform a test, see *Test External Backup and Restore* on page 325.

Remote Appliance Administration

Available only on Aggregator appliances.

These are the options for remote appliances:

- *List Remote Appliances* on page 327
- *Add a Remote Appliance* on page 327
- *Remote Appliance Properties* on page 327
- *Delete a Remote Appliance* on page 328

When to use it When setting up an Aggregator appliance to work with remote appliances.

List Remote Appliances

When to use it When you want to see what remote appliances have been set up to work with this Aggregator.

Effects

- Shows a list that gives the IP address and name of each appliance.
- You can click an appliance on an IP address in the list to go to an Action menu for that specific appliance that allows you to delete the remote appliance from the Aggregator configuration or modify the remote appliance's properties.

Add a Remote Appliance

When to use it

- When setting up an Aggregator to view remote appliances.
- Any time after setup, when you want to add another remote appliance to the setup.

Effects Makes a remote appliance available for viewing from an Aggregator.

Limits The IPv4 address must be valid.

The name must be 2-200 characters long.

Procedural alerts Enter the IP address of the remote appliance and a name for the appliance.

Remote Appliance Properties

Customizes the identification, collection of data and proxy configuration for an appliance that you will view through an Aggregator.

When to use it When you are setting up or changing what appliances will be viewed through an Aggregator, how they will be viewed and by whom.

Effects

- controls what remote appliance will be used as a source of data for the Health Panel
- controls what name will be displayed in the Toolbar appliance list, the Remote Appliance page and so on
- which account name will be used to retrieve data from the remote appliance

- how frequently data is collected from the remote appliance for the local appliance
- how proxy services navigate any firewalls between your management workstation and the devices that Network Discovery has discovered

Options

- appliance IPv4 address
- name
- remote account
- maximum update interval for:
  - health data
  - inventory data
  - events data
  - workstation inventory
- http and telnet proxy configuration:
  - no proxy
  - proxy via local appliance
  - proxy via local appliance and remote appliance
  - proxy via remote appliance

Procedural alerts

Leave the account name blank so you do not automatically retrieve data from a remote system.

Delete a Remote Appliance

When to use it

When you no longer want to see the remote appliance from the Aggregator.

Effects

Removes the remote appliance from the Aggregator setup, so that you will no longer be able to view it remotely.

Does not affect the function of the appliance as an individual appliance.

Limits

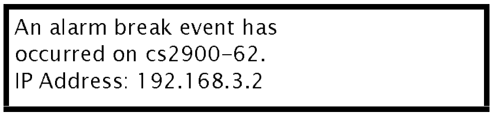
Network Discovery asks you to confirm that you want to delete the remote appliance. You cannot undo the deletion.

Notification and Events Configuration

Here are the notification/events options:

- *Pager Service Provider Configuration* on page 329
- *SNMP Trap Recipient Configuration* on page 334
- *Event Filter Configuration* on page 337

Figure 20-4: Sample pager message



```
An alarm break event has
occurred on cs2900-62.
IP Address: 192.168.3.2
```

Pager Service Provider Configuration

These are the provider options:

- *List Service Providers* on page 330
- *Add a Service Provider* on page 331
- *Service Provider Properties* on page 332
- *Delete a Service Provider* on page 333
- *Modem Properties* on page 333
- *Test Service Provider* on page 333

Important: You must attach an external modem to the Peregrine appliance for pages to be sent (unless an e-mail gateway is used). See the *Setup Guide*.

Important: Only alpha-numeric pagers are supported. Numeric pagers are not supported.

This menu allows you to construct a list of pager service providers local to your area. You must obtain some data from each service provider, and use that data to build a provider profile. It is up to the Network Discovery Administrator to create and test these profiles. Each account will then select one of these provider profiles.

Note: If all accounts are notified of pages through a pager e-mail gateway, you will not need this menu.

Other forms of event notification, such as e-mail, are also available. See *Event Filter Configuration* on page 337.

List Service Providers

Displays a list of existing pager service provider profiles, sorted alphabetically by service name. Includes the service name, data bits, parity, stop bits, baud rate, dialer number, protocol, and profile visibility.

Note: Initially, this list will be empty.

The service names are hyperlinked. The hyperlinks will take you to the shortcut menu for that profile's *Service Provider Properties* on page 332.

To modify a provider profile:

- Click a service name hyperlink.

Add a Service Provider

Adds a new profile for a pager service provider.

Table 25: Service provider profile options

Option	Default	Values	Limits
Service name	—	valid characters	A–Z, a–z*, 0–9, _ (*underscore*)†
	—	length of input (characters)	1–35
Data bits	8	—	5 | 6 | 7 | 8
Parity	Even	—	Even | Odd | None
Stop bits	1	—	1 | 2
Baud rate	300	—	300 | 1200 | 2400 | 4800 | 9600
Dialed number	—	valid characters	0–9
	—	length of input	1–35
Protocol	TAP	—	ANSWER | ATT_WEB | CELLNET_WEB | CIMD | GENERIC | KPN | LIBERTEL | MOBISTAR | MTN | NEXTEL_WEB | ONE2ONE | ORANGE | ORANGE_WEB | PAGENET_WEB | PAGEONE | PROXIMUS | PROXIMUS_WEB | SNPP | TAP | TAP_VARIANT1 | TIM | UCP | UCP_TCP | VODACOM | VODAFONE | VODAPAGE_BLOCK
Description	—	valid characters	A–Z, a–z, 0–9, *all punctuation*, *space*
	—	length of input (characters)	0–80
Enabled	NO		NO | YES

* Alphabetic characters are automatically converted to lower case.

† You may not put underscore characters at the beginning or end of the name. You may not have two underscore characters in a row.

- Service name: the filename for the provider profile
- Data bits, parity, stop bits, baud rate: technical information necessary to connect to the service provider
- Dialed number: the telephone number one must dial to send a page to the provider
- Protocol: technical information necessary to send a page to the provider
- Description: a longer description of the provider profile than is possible with the service name
- Enabled: controls whether or not the provider profile is visible to accounts

Procedural alerts

- Do not include a hyphen in the dialed number.
- Any upper case letters in the service name will be converted to lower case.
- By default, profiles are *not* enabled.

Service Provider Properties

Modifies the profile of an existing pager service provider.

Table 26: Service provider profile options

Option	Default	Values	Limits
Data bits	8	—	5 | 6 | 7 | 8
Parity	Even	—	Even | Odd | None
Stop bits	1	—	1 | 2
Baud rate	300	—	300 | 1200 | 2400 | 4800 | 9600
Dialed number	—	valid characters	0–9
	—	length of input	1–35
Protocol	TAP	—	ANSWER | ATT_WEB | CELLNET_WEB | CIMD | GENERIC | KPN | LIBERTEL | MOBISTAR | MTN | NEXTEL_WEB | ONE2ONE | ORANGE | ORANGE_WEB | PAGENET_WEB | PAGEONE | PROXIMUS | PROXIMUS_WEB | SNPP | TAP | TAP_VARIANT1 | TIM | UCP | UCP_TCP | VODACOM | VODAFONE | VODAPAGE_BLOCK
Description	—	valid characters	A–Z, a–z, 0–9, *all punctuation*, *space*
	—	length of input (characters)	0–80
Enabled	NO	—	NO | YES

- Data bits, parity, stop bits, baud rate: technical information necessary to connect to the service provider
- Dialed number: the telephone number one must dial to send a page to the provider
- Protocol: technical information necessary to send a page to the provider
- Description: a longer description of the provider profile than is possible with the service name
- Enabled: controls whether or not the provider profile is visible to accounts

Procedural alerts

- You cannot change the service name for the provider.
- Do not include a hyphen in the dialed number.

Delete a Service Provider

Deletes the profile of an existing pager service provider.

Modem Properties

For details on modifying the modem initialization string, consult the AT command set documentation that came with your modem.

The dial prefix is for those situations where you must prefix the telephone number you are dialling. For example, it is common to have to dial 9 to get an external line. You can use commas to act as a pause.

Limits

0–47 characters

Default

- Modem initialization string: L3&K0&M0
- Dial prefix: (n/a)

Note: The default modem string should turn the speaker volume high, disable data compression and disable error control

Test Service Provider

Tests the profile of a pager service provider. Allows you to enter the number of a pager.

Requires a pager and pager number associated with the service provider.

The test message you should receive is “Test page from Network Discovery”.

Limits

- *valid characters:* 0–9
- *length of input:* 1–15 characters

Procedural alerts

If an error occurs and you do not receive the page, it could be because:

- incorrect pager data is provided in the provider profile
- incorrect pager ID has been entered
- no external modem is connected to the Peregrine appliance
- the external modem connected to the Peregrine appliance is turned off
- there are modem synchronization problems
- there is no dial tone on the phone line being used
- your service provider is having problems
- your pager is turned off

Related

Each account can also test the pager number and pager service provider associated with the account—see *Test Pager Number* on page 289.

SNMP Trap Recipient Configuration

These are the recipient options:

- *List Recipients* on page 334
- *Add a Trap Recipient* on page 335
- *Modify a Recipient* on page 335
- *Delete a Recipient* on page 335
- *Test a Recipient* on page 336

Network Discovery can generate an SNMP trap based on any event filter. These traps can be exported to a third-party application, for example HP OpenView. These third-party applications are called recipients.

You can have multiple recipients. You will need for the device running the application:

- an IP address or domain name
- a community string

For technical details, contact your Peregrine Systems Customer Support representative.

Technical SNMPv2c notification-type messages

List Recipients

Displays a list of existing recipients, sorted alphabetically by recipient name. Includes the name, device (IP address or domain name), community string, and description.

Note: Initially, this list will be empty.

The service names are hyperlinked. The hyperlinks will take you to the *Modify a Recipient* on page 335, mini-menu for that profile.

To modify a provider profile:

▶ Click a service name hyperlink.

Add a Trap Recipient

Adds a recipient for SNMP traps generated by a Network Discovery event filter. (The event filter must specify the creation of SNMP traps.)

Table 27: Trap recipient options

Option	**Limits**	
	Valid characters	**Input length (characters)**
Recipient name	A–Z, a–z, 0–9, _ *(underscore)**	l1–30
Description	A–Z, a–z, 0–9, *all punctuation except* \ *(backslash), space*	1–255
Host	A–Z, a–z, 0–9, - *(hyphen)*, . *(period)*	1–255
Community	A–Z, a–z, 0–9, *all punctuation except* \ *(backslash), space*	1–35

* You may not put underscore characters at the beginning or end of the name. You may not have two underscore characters in a row.

Modify a Recipient

Modifies the data for a recipient.

Table 28: Trap recipient options

Option	**Limits**	
	Valid characters	**Input length (characters)**
Description	A–Z, a–z, 0–9, *all punctuation except* \ *(backslash), space*	1–255
Host	A–Z, a–z, 0–9, - *(hyphen)*, . *(period)*	1–255
Community	A–Z, a–z, 0–9, *all punctuation except* \ *(backslash), space*	1–35

Procedural alerts

You cannot change the name of the recipient.

Delete a Recipient

Deletes a recipient of SNMP traps.

Test a Recipient

Tests a selected recipient of SNMP traps.

You must have a SNMP trap process running on the recipient. The test trap will begin similarly to the example below:

2001-05-22 15:48:55 nmserver.example.com [192.168.5.2]: system.sysUpTime.0 = Timeticks: (174699469) 20 days, 5:16:34.69

This will be followed by several MIB objects and their values, for example:

enterprises.1467.100.100.1.2.5.6 = "TEST: nmserver.example.com"

Event Filter Configuration

These are the event filter options:

- *List Filters* on page 338
- *Reset to Defaults* on page 338
- *Add a Device Filter* on page 339
- *Add a Line Filter* on page 340
- *Modify a Filter* on page 341
- *Delete a Filter* on page 342

Event filters control two things:

- notification of events
- the event log

The event log controls what you see in Events Browser—see *Chapter 16, Events Browser*.

Notification includes:

- notifying accounts
  - by e-mail
  - by an alphanumeric page
  - by an alphanumeric page through an e-mail gateway
- notifying other systems—SNMP traps (see *SNMP Trap Recipient Configuration* on page 334)
- logging the event in the Network Discovery events database for you to view with the Events Browser

Important: Event filters depend on the priority in the Prime configuration.

Note: Event Filter Configuration does not affect events as displayed in the Health Panel and Network Map.

There are two types of event filters, device filters and line filters. Both filter types are automatically combined when viewed with the Events Browser.

Related For an overview of the paging process, see the *User Guide*.

List Filters

Lists all event filters. The list is sorted alphabetically by filter name.

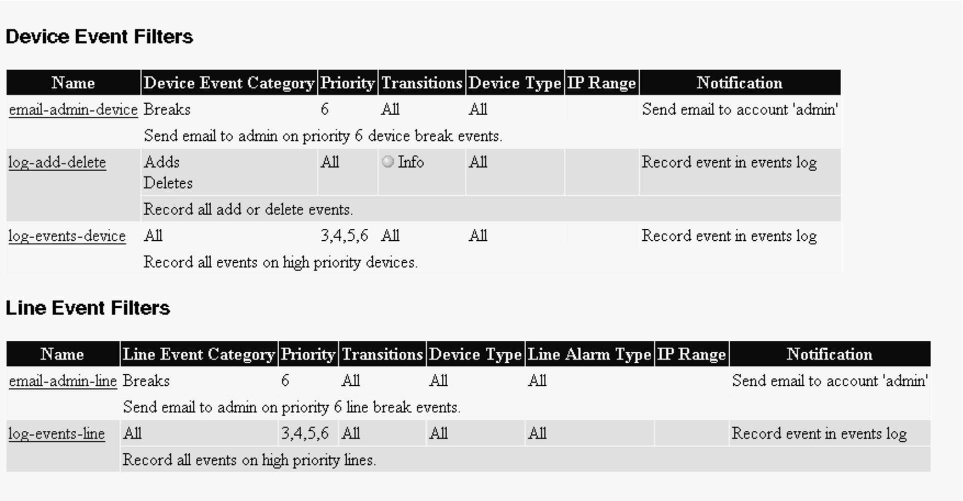
The filter names are hyperlinked. Clicking the hyperlinks will take you to *Modify a Filter* on page 341.

Default

There are five default filters:

- email-admin-device, which sends e-mail to the account named “admin” for breaks on priority 6 devices
- email-admin-line, which sends e-mail to the account named “admin” for breaks on priority 6 lines
- log-events-device, which records all events on devices with high priority (3–6)
- log-events-line, which records all events on lines with high priority (3–6)
- log-add-delete, which records all add or delete events—of any priority (1–6)

Figure 20-5: Default event filters



Device Event Filters

Name	Device Event Category	Priority	Transitions	Device Type	IP Range	Notification
email-admin-device	Breaks	6	All	All		Send email to account 'admin'
	Send email to admin on priority 6 device break events.					
log-add-delete	Adds Deletes	All	○ Info	All		Record event in events log
	Record all add or delete events.					
log-events-device	All	3,4,5,6	All	All		Record event in events log
	Record all events on high priority devices.					

Line Event Filters

Name	Line Event Category	Priority	Transitions	Device Type	Line Alarm Type	IP Range	Notification
email-admin-line	Breaks	6	All	All	All		Send email to account 'admin'
	Send email to admin on priority 6 line break events.						
log-events-line	All	3,4,5,6	All	All	All		Record event in events log
	Record all events on high priority lines.						

Note: If you delete the account “admin”, as suggested to improve your security, be sure to modify or delete the default “email-admin” filters.

Reset to Defaults

Warning: You will delete all the event filters you have created. This action cannot be undone.

Deletes all added or modified event filters, and restores the default filters:

- email-admin-device
- email-admin-line
- log-events-device
- log-events-line
- log-add-delete

Add a Device Filter

Adds a device event filter. A device event filter consists of:

- Selection Criteria (which events and which device types you want to monitor)
- Notification (what you want to happen if an event that meet the criteria occurs)

Each filter must consist of at least one notification. There can be many notifications per filter.

You can restrict a filter to a specific IP range. By default, filters apply to all devices in scope.

Table 29: Event filter options

Option	Default	Values	Limits
Name	—	valid characters	a–z, 0–9*, - *(hyphen)*, _ *(underscore)*
	—	length of input (characters)	3–20
Description	—	valid characters	A–Z, a–z, 0–9, *(space)*, *(most punctuation, excluding single quote)*
	—	length of input (characters)	0–60
Device Event Category	All	—	All | Breaks | Packet Loss | Adds | Deletes
Priority	All	—	All | 1 | 2 | 3 | 4 | 5 | 6
Transitions	All	—	All | OK -> Warning | OK -> Alarm | Warning -> OK | Warning -> Alarm | Alarm -> OK | Alarm -> Warning |Info†
Device Type	All	—	see **Help** > **Device Types**
IP Ranges‡	—	—	0–9, . *(period)*
Notifications	—	—	E-mail | Alphanumeric Page | Alphanumeric Page (via e-mail gateway) | SNMP Trap | Log

* Also, the first character must be letter or number.

† Info comprises Add and Deletes.

‡ The IP address specified is compared against what Network Discovery considers to be the device’s primary IP address.

Procedural alerts

- Any letters in the filter name must be lower case (a–z).
- When using Selection Criteria list boxes, you can select multiple options. *Windows users:* Hold down the Shift or Control key as you click the mouse.
- Selection criteria apply to all notifications.
- You may have multiple notifications per filter.
- If you do not specify an IP range for a filter, it applies to all devices in scope.
- If a device has multiple IP addresses, be sure to determine its primary IP address when specifying the event IP range.

Add a Line Filter

Adds a line event filter. A line event filter consists of:

- Selection Criteria (which events and which line types—connected to which device types—you want to monitor)
- Notification (what you want to happen if an event that meet the criteria occurs)

Each filter must consist of at least one notification. There can be many notifications per filter.

You can restrict a filter to a specific IP range. By default, filters apply to all lines connected to devices in scope.

Table 30: Event filter options

Option	Default	Values	Limits
Name	—	valid characters	a–z, 0–9*, - *(hyphen)*, _ *(underscore)*
		length of input (characters)	3–20
Description	—	valid characters	A–Z, a–z, 0–9, *(space)*, *(most punctuation, excluding single quote)*
		length of input (characters)	0–60
Line Event Category	All	—	All | Breaks | Utilization | Delay | Collisions | Broadcasts | Errors
Priority	All	—	All | 1 | 2 | 3 | 4 | 5 | 6
Transitions	All	—	All | OK -> Warning | OK -> Alarm | Warning -> OK | Warning -> Alarm | Alarm -> OK | Alarm -> Warning
Device Type†	All	—	see **Help** > **Device Types**
Line Alarm Type	All	—	see Table 12 on page 224‡
IP Ranges**	—	—	0–9, . *(period)*
Notification	—	—	E-mail | Alphanumeric Page | Alphanumeric Page (via e-mail gateway) | SNMP Trap | Log

* Also, the first character must be letter or number.
† Optional: You may specify the type of device to which a line is connected.
‡ Exception: “No Alarms” is not available.
** The IP address specified is compared against what Network Discovery considers to be the device’s primary IP address.

Procedural alerts

- Any letters in the filter name must be lower case (a–z).
- When using Selection Criteria list boxes, you can select multiple options. *Windows users:* Hold down the Shift or Control key as you click the mouse.
- Selection criteria apply to all notifications.
- You may have multiple notifications per filter. If you do not specify an IP range for a filter, it applies to all lines connected to devices in scope.
- If a device has multiple IP addresses, be sure to determine its primary IP address when specifying the event IP range.

Modify a Filter

Modifies an existing event filter, whether it is a device filter or a line filter.

An event filter consists of:

- Selection Criteria (which events and which device or line types you want to monitor)
- Notification (what you want to happen if an event that meet the criteria occurs)

The type of filter restricts the available selection criteria. You can have more than one notification per filter.

You can restrict a filter to a specific IP range. By default, filters apply to all lines connected to devices in scope.

Table 31: Device event filter options

Option	Default	Values	Limits
Description	—	valid characters	A–Z, a–z, 0–9, *(space), (most punctuation, excluding single quote)*
	—	length of input (characters)	0–60
Device Event Category	All	—	Breaks | Packet Loss | Adds | Deletes
Priority	All	—	All | 1 | 2 | 3 | 4 | 5 | 6
Transitions	All	—	All | OK -> Warning | OK -> Alarm | Warning -> OK | Warning -> Alarm | Alarm -> OK | Alarm -> Warning | Info*
Device Type	All	—	see **Help** > **Device Types**
IP Ranges†	—	—	0–9, . *(period)*
Notification	—	—	E-mail | Alphanumeric Page | Alphanumeric Page (via e-mail gateway) | SNMP Trap | Log

* Info comprises Add and Deletes.

† The IP address specified is compared against what Network Discovery considers to be the device’s primary IP address.

Table 32: Line event filter options

Option	Default	Values	Limits
Description	—	valid characters	A–Z, a–z, 0–9, *(space)*, *(most punctuation, excluding single quote)*
		length of input (characters)	0–60
Line Event Category	All	—	Breaks | Utilization | Delay | Collisions | Broadcasts | Errors |
Priority	All	—	All | 1 | 2 | 3 | 4 | 5 | 6
Transitions	All	—	All | OK -> Warning | OK -> Alarm | Warning -> OK | Warning -> Alarm | Alarm -> OK | Alarm -> Warning | Info
Device Type*	All	—	see **Help** > **Device Types**
Line Alarm Type	All	—	see Table 12 on page 224
IP Ranges†	—	—	0–9, . *(period)*
Notification	—	—	E-mail | Alphanumeric Page | Alphanumeric Page (via e-mail gateway) | SNMP Trap | Log

* Optional: You may specify the type of device to which a line is connected.
† The IP address specified is compared against what Network Discovery considers to be the device's primary IP address.

Procedural alerts

- You cannot change the name for a filter.
- When using Selection Criteria list boxes, you can select multiple options. *Windows users:* Hold down the Shift or Control key as you click the mouse.
- Selection criteria apply to all notifications.
- You may have multiple notifications per filter.
- You may have multiple notifications per filter. If you do not specify an IP range for a filter, it applies to all devices in scope, or to all lines connected to devices in scope.
- If a device has multiple IP addresses, be sure to determine its primary IP address when specifying the event IP range.

Delete a Filter

Delete an event filter from Network Discovery.

Advanced Administration

Here are the advanced options

- Network Tuning
- *Appliance Services* on page 356
- *Data Management* on page 360
- *Router Discovery* on page 365
- *Display Preferences* on page 368
- *Device Manager Ports Display Preferences* on page 376

Network Tuning

Configures advanced values and overrides that control the collection of network data.

Important: The items in this menu are for experienced users only.

These are the tuning options:

- *Input Filters* on page 343
- *XML Enricher configuration* on page 348
- *Network Management* on page 349
- *Expiry* on page 352
- *Overrides* on page 354

Input Filters

Determines which devices are permitted in the Network Discovery database.

When to use it

A filter allows you to reduce the number of devices in your Network Map. Common uses for filters:

- to remove from the Network Map devices you do not wish to monitor
- to reduce the number of devices applied against your device license

You may want certain classes of device to be part of the database only when their existence has been confirmed.

The options for Input Filters that allow certain classes of device to be part of the database only when their existence has been confirmed are:

- *Time for which a filtered MAC plus IP device is valid* on page 344
- *Time in which MAC-only device must be seen twice* on page 344
- *Time in which an accumulated IP address must be reconfirmed* on page 345
- *MAC-only devices must be seen by at least two devices* on page 345

You may want to prevent certain classes of device from being added to the database.

The options for Input Filters that prevent certain classes of device from being added to the database are:

- *Unmanaged devices which are MAC plus IP* on page 346
- *Unmanaged devices which are MAC plus IP and not pingable* on page 346
- *Unmanaged devices which are MAC-only* on page 346
- *Unmanaged devices which are MAC-only with unknown OUIs* on page 346
- *Unmanaged devices which are IP-only* on page 347
- *Scanned-only devices* on page 347

Procedural alerts

Check boxes that are indented are a subset of the check box immediately above. You can check an indented check box without checking the previous check box.

Related commands

For a list of the devices that are currently being filtered, see **Status** > **Filtered Devices**.

Time for which a filtered MAC plus IP device is valid

Determines the length of time Network Discovery waits before it purges an expired IP/MAC pair from the database.

Shorter intervals allow more MAC-only objects to become discovered.

When to use it

Effects

If you have a device (an IPv4 range) set up to be avoided, shortening the time allows the MAC address that was associated with the IP to become active. These IP/MAC pairs typically come from ARP entries and allow MAC-only devices to be blocked when associated with an IP address that is set up to be avoided.

Limits

Note: This interval is only used if the IP address associated with the MAC is outside the IPv4 address ranges set up for discovery.

Default

The default interval is 7 days.

Related commands

For a list of the devices that are currently being filtered, see **Status** > **Filtered Devices**.

Time in which MAC-only device must be seen twice

Determines the length of time that Network Discovery can take to confirm the existence of a MAC-only device (after its initial detection). Unconfirmed devices will never appear on the Network Map.

Shorter intervals permit fewer MAC-only objects to be added to the database.

Once a MAC-only device has been confirmed, it stays on the Network Map until the device is disconnected from the network. After the device is confirmed, Network Discovery ignores the interval for that device.

When to use it

If Network Discovery is displaying several MAC-only devices that you know are non-existent, use a shorter interval. If Network Discovery is not displaying several MAC-only devices that you know are connected to your network, use a longer interval to give Network Discovery extra time to confirm devices.

Limits

Note: If "Unmanaged devices which are MAC-only" is checked, the value for this interval is ignored.

Default

The default interval is 2 days.

Related commands

For a list of the devices that are currently being filtered, see **Status** > **Filtered Devices**.

Time in which an accumulated IP address must be reconfirmed

Determines the length of time Network Discovery waits before it removes an expired IP address associated with the unmanaged router. This allows router configurations to be updated more frequently. These unmanaged router IP addresses typically come from ARP entries.

Shorter intervals update an unmanaged router more frequently.

Limits

Note: This interval is only used if at least one of the router IP addresses has been included in the list of *Unmanaged Routers*.

Default

The default interval is 1 week (7 days).

Related commands

For a list of the devices that are currently being filtered, see **Status** > **Filtered Devices**.

MAC-only devices must be seen by at least two devices

Determines whether MAC-only devices must have been detected by two separate network devices. (Note that this is *not* related to a MAC-only device having been seen twice by the same device.)

A filter allows you to reduce the number of devices in your Network Map. Common uses for filters:

- to remove from the Network Map devices you do not wish to monitor
- to reduce the number of devices applied against your device license

Check boxes that are indented are a subset of the check box immediately above. You can check an indented check box without checking the previous check box.

When to use it

You may want to prevent certain classes of device from being added to the database.

Effects

If set to **Yes**, MAC-only devices that have not been confirmed by two devices never appear on the Network Map.

Limits

Note: If "Unmanaged devices which are MAC-only" is checked, the value for this option is ignored.

Default

The default value is **Yes**.

Related commands

For a list of the devices that are currently being filtered, see **Status** > **Filtered Devices.**

Unmanaged devices which are MAC plus IP

Determines whether devices with no SNMP agent but with both a MAC address and an IP address will appear on the Network Map.

Default

The default state is clear (which allows these devices to be added).

Procedural alerts

Check boxes that are indented are a subset of the check box immediately above. You can check an indented check box without checking the previous check box.

Related commands

For a list of the devices that are currently being filtered, see **Status** > **Filtered Devices.**

Unmanaged devices which are MAC plus IP and not pingable

Determines whether devices with no SNMP agent but with both a MAC address and an IP address will appear on the Network Map when these devices do not respond to ping requests.

The default state is clear (which allows these devices to be added).

Procedural alerts

Check boxes that are indented are a subset of the check box immediately above. You can check an indented check box without checking the previous check box.

Related commands

For a list of the devices that are currently being filtered, see **Status** > **Filtered Devices.**

Unmanaged devices which are MAC-only

Determines whether devices with only a MAC address (that is, no SNMP agent and no IP address) will appear on the Network Map.

The default state is clear (which allows these devices to be added).

Procedural alerts

Check boxes that are indented are a subset of the check box immediately above. You can check an indented check box without checking the previous check box.

Related commands

For a list of the devices that are currently being filtered, see **Status** > **Filtered Devices.**

Unmanaged devices which are MAC-only with unknown OUIs

Determines whether devices with only a MAC address (that is, no SNMP agent and no IP address) and with an OUI that Network Discovery does not recognize will appear on the Network Map.

The Organization Unique Identifier (OUI) is the first three octets of a MAC address, and identifies the organization that manufactures the device associated with the MAC address. If the OUI is in the Network Discovery database, then the first three numeric octets are replaced by an abbreviation of the organization's name (e.g. "KINGST12685B"). If the OUI is unknown to Network Discovery, all octets of the OUI are displayed numerically (e.g. "F801001A0060").

Included in the set of hidden MAC addresses are:

- false MAC addresses generated by switches with multicast entries in their bridge tables
- corrupted MAC addresses produced by repeaters with problems performing source address capture

If you choose to show devices with false and garbled MACs, they will appear on your Network Map with "Unknown" icons.

The default state is clear (which allows these devices to be added).

Procedural alerts Check boxes that are indented are a subset of the check box immediately above. You can check an indented check box without checking the previous check box.

Related commands For a list of the devices that are currently being filtered, see **Status** > **Filtered Devices**.

Unmanaged devices which are IP-only

Determines whether devices with only an IP address (that is, no SNMP agent and no IP address) will appear on the Network Map. Any such devices are initially given pseudo MAC addresses. If the correct address is determined, the model will be updated to include the genuine MAC address.

Limits **Note:** Use this option with care in networks that rely on DHCP.

Default The default state is checked (which prevents these devices from being added).

Procedural alerts Check boxes that are indented are a subset of the check box immediately above. You can check an indented check box without checking the previous check box.

Related commands For a list of the devices that are currently being filtered, see **Status** > **Filtered Devices**.

Scanned-only devices

Determines whether or not Network Discovery collects and presents devices known only from scan file data.

Default Not checked (Network Discovery does *not* collect and present devices known only from scan file data).

Procedural alerts

Check boxes that are indented are a subset of the check box immediately above. You can check an indented check box without checking the previous check box.

Related commands

For a list of the devices that are currently being filtered, see **Status** > **Filtered Devices**.

XML Enricher configuration

You can configure the xml enricher to merge scanned device information into the databases. Optionally, you can generate files for import into Microsoft's System Management Server software.

The options for XML Enricher configuration are:

- *Generate MIF files.* on page 348
- *Automatically defer all new scans* on page 348

Generate MIF files.

When to use it

When you want to use scan files with Microsoft's System Management Server software.

Options

The options for when Network Discovery should generate MIF files are:

- Always
- Never
- When SMS is detected (When Microsoft's System management Server software is detected).

Limits

Only for use with Peregrine's Express Inventory (the WMI collector). For information on setting up and using the WMI collector, see your Service Center Essentials documentation.

Default

Never

Procedural alerts

Changes do not take effect until you click the **Change** button.

Automatically defer all new scans

Options

Yes or No

Limits

Only for use with Peregrine's Express Inventory (the WMI collector). For information on setting up and using the WMI collector, see your Service Center Essentials documentation.

Default

No

Procedural alerts

Changes do not take effect until you click the **Change** button.

Network Management

Set rates for pinging, polling, and table reading.

The Network Management options are:

- *Ping* on page 349
- *Table Reader* on page 350
- *Device Poller* on page 350
- *Resource Poller* on page 351

When to use it

Rarely. When you want to alter the balance between putting overhead on the network and getting the maximum amount of information. Before you change the rates, make sure Network Discovery is performing discovery as efficiently as possible in **Administration** > **Network configuration** > **Add IPv4 range**

Effects

Lowering the rates decreases traffic on the network, but it also means that data updates less frequently.

Procedural alerts

Important: Each of these rates will be ignored if the corresponding process in **Administration** > **Network Tuning** > **Overrides** is set to **No** (see *Overrides* on page 354.

Related commands

Status > **Current settings** > **Network Tuning** shows how Network Tuning is currently set.

Ping

Ping rate controls the maximum number of IP addresses that are pinged each second. Network Discovery may ping at a lower rate than that specified.

Ping rate affects not only the speed at which your network is discovered but the amount of network overhead—that is, the amount of traffic Network Discovery generates.

Pinging an address at which no device exists can create more traffic, not less, because Network Discovery keeps trying. Some routers in your network may ARP multiple times for a ping that produces no reply. (Network Discovery itself ARPs once for a ping, regardless of whether it produces a reply.) This means that in a network with a address range lightly populated with devices, the ARP rate might be 3–4 times greater than the ping rate.

Tip: To speed up initial discovery, you may increase the ping rate to 10.0–20.0. However, if you do so, monitor your network the whole time the rate is set at 10.0 or higher.

You may return the rate to 5.0 or lower once most of your devices have been discovered. This will reduce traffic on your network. In a stable network, a value of 1 or less is normal.

Important: If you set the ping rate to 10.0 or higher, broadcast traffic may increase to an unacceptable level in some networks.

Effects Lowering the rates decreases traffic on the network, but it also means that data updates less frequently.

Limits 0.01 to 100 pings per second

Default 5.0 pings per second

Procedural alerts

Important: Ping rate will be ignored if > **Network Tuning** > **Overrides** > **Ping active** is set to **No** (see *Overrides* on page 354).

Related commands **Status** > **Current Settings** > **Network Tuning** > **Ping Rate** shows what ping rate is currently set.

Table Reader

Table reader rate controls the maximum number of times that bridge tables and ARP tables are polled and read each second. Network Discovery may poll tables at a lower rate than that specified.

Effects Lowering the rates decreases traffic on the network, but it also means that data updates less frequently.

Limits 0.1 to 100.0 polls per second

Default 10 polls per second

Technical Network Discovery will normally use SNMP bulkwalk during table reading. If you notice high CPU on your routers or switches, decrease the table reader rate and contact Peregrine customer support.

Procedural alerts

Important: Table reader rate will be ignored if **Administration** > **Network Tuning** > **Overrides** > **Table reader active** is set to **No** (see *Overrides* on page 354).

Related commands **Status** > **Current Settings** > **Network Tuning** > **Table reader rate**

Device Poller

Device poller rate controls the maximum number of devices that are polled for statistics each second. Network Discovery may poll at a lower rate than that specified.

Effects

Lowering the rates decreases traffic on the network, but it also means that data updates less frequently.

Options

0.5 to 100 polls per second

Limits

Lowering the Device poller rate increases the poll interval. If you lower the poller rate so much that the poll interval exceeds 60 minutes, the Network Mapper will stop running.

Default

30 polls per second

Procedural alerts

Important: Device poller rate will be ignored if **Administration** > **Network Tuning** > **Overrides** > **Device poller active** is set to **No** (see *Overrides* on page 354.

Related commands

Status > **Current Settings** > **Network tuning** > **Device poller rate** shows how Device poller rate is currently set.

Resource Poller

The resource poller rate controls the maximum number of devices that are polled for resource data each second. Network Discovery may poll at a lower rate than that specified.

Effects

The resource poller rate affects the amount of traffic Network Discovery generates.

Limits

0.1 to 100 polls per second

Default

5.0 polls per second

Procedural alerts

Important: Resource poller rate will be ignored if **Administration** > **Network Tuning** > **Overrides** > **Resource poller active** is set to **No** (see *Overrides* on page 354.

Related commands

Status > **Current Settings** > **Network tuning** > **Resource poller rate** shows how Resource poller rate is currently set.

Expiry

Determines how long before inactive devices are removed from the database. Changes Trash and Purge intervals.

After Network Discovery has determined that it has received no data from a device for a set interval, Network Discovery removes that device from the Network Map—first temporarily, so that its statistical history can be easily recovered if the device resumes operation, and then permanently.

The set intervals are two:

- *Device Trash Intervals* on page 352 how long before a “not seen” is temporarily removed
- *Device Purge Intervals* on page 353 how long before a trashed device is permanently removed

Each type, trash and purge, has separate intervals for:

- managed devices
- unmanaged devices
- devices found only by scan files

This is because Network Discovery tends to communicate with managed devices more frequently.

All intervals should be long enough that devices may be turned off for long periods, but short enough that devices removed from the network are not needlessly monitored.

Device Trash Intervals

Refers to the maximum length of time Network Discovery waits before it moves a "not seen" device into the trash.

Devices in the trash disappear from the Network Map and reports, but their statistical information is preserved in case the devices are made active before they are permanently purged.

Limits

Note: A trash interval may be less than the specified value. The trash has limited capacity (10% of the device license). Once the trash reaches its capacity, some devices will be automatically purged.

The interval for managed devices must be 2 days-12 weeks in length. The interval for unmanaged devices must be 1 day-12 weeks in length.

Default

The default interval for managed devices is up to 8 weeks. The default interval for unmanaged devices is up to 1 week.

Related commands

Note: The trash interval for unmanaged devices is dependant on the Device Modeler Interval. The time it takes to trash an unmanaged device is either the trash interval, or 3 times the Device Modeler Interval, whichever is longer.

For example, if you change the trash interval for unmanaged devices to 1 day, but do not change the default Device Modeler Interval of 2 days, Network Discovery will take 6 days (3 times 2 days) to trash an unseen unmanaged device.

Device Purge Intervals

Refers to the length of time Network Discovery waits before it purges a device that has been moved to the trash.

Note: The purge interval does not begin until the trash interval ends. In other words, the purge interval does not begin until the device is placed in the trash.

Devices that are purged disappear from the Network Map and reports, and their statistical information is destroyed. Contrast this with the trash, in which statistical information is preserved.

Once a device has been purged, it normally remains absent from the Network Map. A purged device may be rediscovered if it is still connected—but it is considered a new device.

Limits

The interval for managed devices must be 1-12 weeks in length. The interval for unmanaged devices must be 1-12 weeks in length.

Default

The default interval for managed devices is 4 weeks. The default interval for unmanaged devices is 4 weeks.

Related commands

Tip: You can also purge a device immediately, without waiting for the purge interval. You can do this from a map window through the **Object** menu, or from the Device Manager.

Overrides

Emergency controls for turning off various parts of Network Discovery

Network Discovery only works properly when all the processes listed below are active. The overrides below should be used for advanced diagnostic purposes only.

Note: If you set any process to No, the corresponding value is ignored. Most values are specified in **Administration** > **Network Tuning** > **Network Management**. The Device Modeler Interval is specified in **Administration** > **Network Configuration** > **Network Property Groups**.

Tip: We recommend that you change these settings only when advised to by your Customer Support representative.

Ping

Emergency control to stop Network Discovery pinging devices.

Ping active determines whether to check for the existence of devices in the address ranges set up for discovery, and whether to establish an association between an IP address and a device.

When to use it

Tip: We recommend that you turn Ping on and off only when advised to by your Customer Support representative.

Default

The default is Yes; Network Discovery pings devices in the address ranges where it is set up to do so.

Related commands

Administration > **Network Tuning** > **Network Management** > **Ping Rate** to set the rate.

Administration > **Network configuration** > **Add IPv4 range** to set up ranges for discovery. Make sure Network Discovery is set up to examine your network as efficiently as possible.

Table Reader

Table reader active determines whether to read the tables of various devices, including the bridge tables of switches and the ARP tables of routers. Data read from tables helps Network Discovery to determine connectivity among devices.

When to use it

Tip: We recommend that you turn Table Reader on and off only when advised to by your Customer Support representative.

Default

The default is Yes; Network Discovery reads tables in the address ranges where it is set up to do so.

Related commands

Administration > **Network Tuning** > **Network Management** > **Table reader rate** to set the rate.

Administration > **Network configuration** > **Add IPv4 range** to set up ranges for discovery. Make sure Network Discovery is set up to examine your network as efficiently as possible.

Device Poller

Device poller active determines whether to poll the devices in the network for traffic statistics and other data.

When to use it

Tip: We recommend that you turn the Device Poller on and off only when advised to by your Customer Support representative.

Tip: If you need to disconnect the Network Discovery appliance from the rest of your network temporarily, set Device poller active to No before disconnecting. Setting Device poller active to No prevents Network Discovery from generating break faults during the time the Network Discovery appliance is disconnected.

Default

The default is Yes; Network Discovery polls devices in the address ranges where it is set up to do so.

Related commands

Administration > **Network Tuning** > **Network Management** > **Device poller rate** to set the rate.

Administration > **Network configuration** > **Add IPv4 range** to set up ranges for discovery. Make sure Network Discovery is set up to examine your network as efficiently as possible.

Resource Poller

Resource poller active determines whether to collect and refresh current resource data from devices in the Resource list.

When to use it

Tip: We recommend that you turn the Resource Poller on and off only when advised to by your Customer Support representative.

Default

The default is Yes; Network Discovery polls resources in the address ranges where it is set up to do so.

Related commands

Administration > **Network Tuning** > **Network Management** > **Resource poller rate** to set the rate.

Administration > **Network configuration** > **Add IPv4 range** to set up ranges for discovery. Make sure Network Discovery is set up to examine your network as efficiently as possible.

Device Modeler

Device modeler active determines whether to interrogate devices that have been discovered by the Network Explorer, and build up device models based on that interrogation.

Device models exist to identify a device, and comprise the following:

- what type of device it is
- what the device's host name is
- how many ports the device has
- what the device's community strings are

When to use it

Tip: We recommend that you turn the Device Modeler on and off only when advised to by your Customer Support representative.

Default

The default is Yes; Network Discovery models devices in the address ranges where it is set up to do so.

Related commands

Administration > **Network configuration** > **Add IPv4 range** to set up ranges for discovery. Make sure Network Discovery is set up to examine your network as efficiently as possible.

Appliance Services

Appliance Services includes:

- *Remote SSH Access* on page 357
- *MySQL Access* on page 357
- *XML Enricher configuration* on page 348
- *Appliance Proxy Services* on page 358
- *Display Warnings* on page 358

Configures user access to the appliance, access given to the appliance, and output about the appliance.

Related

Appliance Management on page 293

Remote SSH Access

Controls whether Network Discovery allows Peregrine Customer Support to login through SecureShell (SSH).

When to use it

At Startup to allow Peregrine Systems Customer Support to access your appliance through the ethernet interface.

SSH access is required for support no matter which option you choose for Peregrine access to your appliance. The options are:

- internet
- through a Virtual Private network over the Internet
- by a modem and a dedicated analog telephone line
- through a Remote Access Server (RAS)

Default

The default is Enabled

Related

Tip: If your network security policy does not permit remote dial-up access to the Peregrine appliance, do not attach a phone line to the internal modem.

To allow Peregrine Systems Customer Support SSH access to your appliance through the Internet, a VPN or a RAS, you must also enable port 22/tcp in your corporate firewall from sprocket.loran.com (209.167.240.9).

MySQL Access

Access to the Network Discovery MySQL database is required only when you intend to create customized reports. Network Discovery can always access its own database, but a third-party report generator cannot make use of the Network Discovery MySQL database until access is enabled. There is more information on how to create custom reports with your own data access application in the *Data Export Guide*.

Limits

- For you to take advantage of this, access to the MySQL database must be granted to at least one account. See Account Properties for detailed instructions.

Default

Disabled.

Related commands

You must also grant access to the MySQL database to at least one account. See *Account Properties* on page 309 for details.

XML Enricher Access

When you disable the XML enricher, the scan files queue up in the shared directory. This allows you to validate the data before the enricher submits it to the database.

Limits

This command is only relevant if you are using Peregrine's Express Inventory (the WMI collector). For information on setting up and using the WMI Collector, see your ServiceCenter Essentials documentation.

Default

By default the XML enricher is enabled (set to Yes).

Related commands

For an account to be able to validate the data, an Administrator must have set the account's Shared directory access to **Yes** in **Administration** > **Account administration** > **Account properties**. (See *Account Properties* on page 309.)

Appliance Proxy Services

Appliance proxy services control how each appliance—whether an Aggregator or remote appliance—directs and redirects certain processes, such as Telnet and HTTP.

For proxy configuration to work correctly, every appliance must have its proxy services set correctly (see *Remote Appliance Administration* on page 327).

This is an advanced feature.

Note: The option "Enable proxy services and use them" is for advanced users only, and should only be used after consultation with Peregrine Systems Customer Support.

Default

Disable proxy services

Display Warnings

Controls whether Network Discovery generates a warning when key pieces of hardware are not attached to the Peregrine appliance or when scheduled backups are not occurring.

We strongly recommend the use of a UPS, access to constant customer support and regular backups. For that reason, if Network Discovery detects that devices you need for these processes are absent, or that scheduled backups are not occurring, Network Discovery creates a warning condition. This warning affects your Health Panel display as well.

When to use it

Rarely. At setup. Disable the warnings when you have other solutions and do not need the hardware or the backups.

UPS Warnings

Controls whether Network Discovery generates a warning when it detects that there is no UPS.

We strongly recommend the use of a UPS (Uninterruptible Power Supply) with your Network Discovery appliance. For that reason, if Network Discovery detects that no UPS is present, Network Discovery creates a warning condition for *Appliance Health*.

When to use it

Rarely. At setup. If you will not be connecting a UPS directly to your Network Discovery appliance, you may choose to have Network Discovery suppress this warning.

Default

The default is Yes.

Modem Warnings

Controls whether Network Discovery generates a warning when it detects that there is no internal modem.

We strongly recommend that you give Peregrine Systems Customer Support constant access to your Network Discovery appliance. For that reason, if Network Discovery detects that no internal modem is present, Network Discovery creates a warning condition for *Appliance Health*.

When to use it

Rarely. At setup. If you have chosen to receive customer support through:

- the Internet
- over a virtual Private network (VPN)
- over a Remote Access Server (RAS)

and you will not be inserting a PCI modem directly into your Network Discovery appliance, you may choose to have Network Discovery suppress this warning.

Default

The default is Yes.

Backup Warnings

We strongly recommend you configure a backup of your Network Discovery data. For that reason, if Network Discovery detects that you have configured a backup and detects that it has not successfully completed a backup within the past 25 hours, Network Discovery creates a warning condition for *Appliance Health*.

When to use it

Rarely. At setup.

Default

The default is Yes.

Procedural alert

If you have not configured a backup, you do not receive a warning.

Data Management

These are the data management options:

- *Check All Community Strings* on page 360
- *Delete Connections* on page 361
- *Delete Data* on page 362
- *View Data Deletion Logs* on page 363
- *Connect-IT Appliance ID* on page 363
- *Restore Prime Map Configuration* on page 364

It can sometimes be necessary to undo all assumptions Network Discovery has made about the contents of a network and how elements are connected. These are not everyday operations—they are drastic. Drastic as they are, they are sometimes useful. Data management manages and configures the deletion and restoration of internal data.

Check All Community Strings

The next scheduled model update will check the complete list of community strings for all device models.

Network Discovery normally uses the successful, active community string for a device. If Network Discovery checked the complete list of possible community strings each time, it could potentially trigger multiple SNMP traps.

However, if you add a new community string to the list, and that string affects several devices on your network, you may wish to inform all devices of the existence of this new string. This feature allows you to force this global check of community strings.

Tip: If you have changed the community string for one or two devices, use the Device Manager's **Update Model** button instead. **Update Model** also checks the complete list of community strings, but only for a single device.

Delete Connections

Deletes connections between objects on the Network Map. It takes a few moments for the changes to be reflected in the map.

Warning: You can potentially lose all the connectivity data Network Discovery has gathered.

Warning: This action cannot be undone.

You can choose to delete:

- all the connections that have been made, both those that Network Discovery has established and those that have been defined by the user
- just the connections define by the user (by Administrator or IT Manager accounts) with the Port Manager—see *Chapter 12, Port Manager*

When to use it

When you have rearranged your network so much that the existing connection data is more of a hindrance than a help.

Effects

Although only connections data are destroyed, deleting connections may cause packaging to be destroyed (sometimes gradually). You and all other account users must be prepared to reconstruct all packaging and layout if you delete all connections.

If you delete all connections, Network Discovery starts over in its attempts to establish connections between objects. User-defined connections are not be re-established no matter which of the two options you select.

Default

There is no default selection.

Delete Data

Deletes data and statistics for your network stored on your Peregrine appliance. Depending on the option chosen, this feature can also delete data used to configure the appliance.

Warning: This is an extremely drastic action that cannot be undone. You will lose *all* the information Network Discovery has gathered since its first day of operation.

Options

There are three options of increasing severity:

Table 33: Options for deleting data

What gets deleted	Network data	Network data plus accounts	Network data, accounts, config, backups
Devices for this appliance	YES	YES	YES
Events	YES	YES	YES
Forecast databases	YES	YES	YES
Accounts	—	YES	YES
Map configurations	—	YES	YES
Devices for any remote appliances*	—	—	YES
Administration configuration	—	—	YES
Internal backups	—	—	YES

* This applies only when an Aggregator license is present.

Important: "Devices" includes the device itself, any statistical history for the device, events, and any WMI scan files.

- *Network data:* the Network Discovery database of your network devices are deleted, along with device statistics, events, and Forecast databases—and reports and graphs, since they are dependent on statistics
- *Above plus accounts:* everything listed under "Network data", plus accounts and their map configurations
- *Above plus configuration data and internal backup:* everything listed under "Network data and accounts", plus configuration from the Administration menu (for example, appliance configuration, network configuration, etc.) and internal backups.

Procedural alerts

Deleting this data takes 5–10 minutes. while this is happening, Network Discovery does not communicate with your Web browser. This means that you have no feedback on how the process is proceeding.

You have the choice of receiving e-mail with the status of the data deletion.

Note: If your account has an e-mail address associated with it, that will be filled in. You may substitute another e-mail address.

View Data Deletion Logs

Displays when data deletion was requested and the progress of the request, including its success or failure.

Connect-IT Appliance ID

Shows the current Peregrine appliance ID for use with Peregrine's Connect-IT.

An arbitrary number is assigned to each Peregrine appliance for identification purposes. Connect-IT uses the Peregrine appliance number when collecting data from Network Discovery. If you have one Peregrine appliance, you may accept the default value. If you have more than one Peregrine appliance, you must assign each Peregrine appliance a unique number.

Tip: In many networks, the easiest way of ensuring unique Appliance ID numbers is to use the final octet of the IP address for the appliance. For example, if the IP address is 172.17.2.3, then use 3 for the Appliance ID number.

Limits The appliance ID must be a value 1-255.

Default The default is 1.

Restore Prime Map Configuration

Allows the Network Discovery Administrator (or other Administrator account) to restore a Prime configuration from one of the backups on the hard disk of the Peregrine appliance.

Backups are made at the following intervals:

- every 24 hours for the past 7 days
- every Monday for the past 4 weeks
- every first day of the month for the past 12 months

When to use it

You need **Restore Prime Map Configuration** only when Network Discovery tells you that the existing “Prime” configuration has become corrupt

Limits

Can only restore from a backup that contains a Prime configuration.

Router Discovery

These are the options for router discovery:

- *Router Discovery Settings* on page 366
- *Run Router Discovery* on page 367
- *Router Discovery Results* on page 367

Router Discovery is a tool to help you learn what device ranges have been populated in your network. Router Discovery attempts to discover the boundaries of your network without the help of the ranges you have set up for discovery (*Network Configuration* on page 317). It discovers boundaries based on routers and their subnets. You do not need to use this option, if you have set up IPv4 ranges for Network Discovery to discover.

Important: Reserve Router Discovery for when you have absolutely no idea what devices are in your network.

The correct community strings are required for Router Discovery to be successfully completed.

Note: If you do not initiate router-based discovery, Network Discovery still discovers the devices in your network—including the routers—by means of the Network Explorer.

Limits

A maximum of 200 routers can be discovered.

Router Discovery Settings

These settings establish the limits of router discovery. There are two settings:

- Hops: routers must not be more than this many hops away
- Line speed: routers must only use the specified line capacities

Hops

The *Maximum hops* value instructs Network Discovery to query only those routers that are *N* or fewer hops from the Peregrine appliance.

Limits The number of router hops must be 1–100.

Default The default number of hops is 2.

Procedural Alert If set to a value of 1, Network Discovery simply finds the default gateway. Values of 2 or more are more useful.

Important: Increasing the maximum hops substantially increases the time it takes to run router discovery.

Line Speed

The minimum and maximum *Line speed* are used to prevent Network Discovery from traversing routers that specify a line speed outside the given range.

Table 34: Router Discovery Settings defaults

Setting	Limits	Default
Maximum Hops	1–100 hops	2 hops
Minimum Line Speed	0 bits/sec *to* 100 Gbits/sec	10 Mbit/sec
Maximum Line Speed	0 bits/sec *to* 100 Gbits/sec	100 Gbit/sec

When to use it To limit exploration of your network.

Effects

- If you increase the number of router hops, you substantially increase the discovery time for your network.
- The line speed ranges are inclusive. For example, a range of 10 Mbits to 1 Gbits would find all Ethernet routers.
- The line speed values are obtained by Network Discovery from the devices that it queries.
- Some devices report an incorrect line speed. This incorrect value affects both discovery and the accuracy of Utilization statistics.

Procedural alerts

- Network Discovery uses the line speed reported by the router closest (in hops) to the Peregrine appliance.

Run Router Discovery

Initiates automatic discovery of routers and subnets, using the parameters specified in *Router Discovery Settings* on page 366 and community strings (see the *Setup Guide*).

Note: If your account has an e-mail address associated with it, you can click the check box next to the prompt "Send e-mail when completed?". You will then be e-mailed when the results are ready to view.

When the results of the run are ready, they can be seen at *Router Discovery Results*, next.

You must confirm this action. Router discovery takes time to run.

Limits A maximum of 200 routers can be discovered.

Router Discovery Results

Displays the results of a router discovery run. If router discovery has not been run, the results are blank. You can see some results while it is running if you click "refresh" on your browser.

The results include:

- the number of hops from the Peregrine appliance to the router
- the IP address of the router (and its interfaces)
- the subnets and netmasks for each router

You can add the results to any of the property sets (see the *Setup Guide*).

Limits

- 1000 devices

Display Preferences

The display preferences options are:

- *Device Title Preference* on page 369
- *Style Sheet* on page 371
- *Automatic Packaging* on page 372
- *Element Management* on page 374

Configures how data is displayed in various areas of Network Discovery.

Table 35: Display preferences defaults

Setting	Default
Device Title Preference	■ Device-specific title ■ Domain name ■ NetBIOS name (network) ■ NetBIOS name (scan) ■ Asset Tag
Style Sheet	—
Automatic Packaging	all ON
Element Management	—

Device Title Preference

Designates the types of title used to identify devices.

Network Discovery stops as soon as it matches an option for the title; only an unsuccessful search causes Network Discovery to continue to the next ranked item.

Not all data are available for all devices. For example, domain names are unavailable unless you have designated one or more *Domain Name Servers* on page 297. The system description is unavailable if the device manufacturer has not set it, or for devices that are not SNMP-managed.

Some options take precedence over the device title preference:

- user-assigned name
- Prime-assigned name
- *virtual devices only:* Network Discovery generated name

If Network Discovery fails to find data for any of the preferences for a device, that device's title is the first available numeric address for the device:

- IPv6 address
- IPv4 address
- MAC address including OUI
- MAC address (all-numeric)

In summary then, the title for a device (real or virtual) is the first available of:

- user-assigned name
- Prime-assigned name
- *virtual devices only:* Network Discovery generated name
- a device title you choose as the Network Discovery Administrator. You can choose one or several of the following and choose their order too:
    - Asset Tag
    - BIOS Asset Tag
    - NetBIOS Name (scan)
    - Last Name
    - First name
    - Device-specific title
    - Domain name
    - NetBIOS name (network)
    - Operating system
    - Family
    - Model
    - Network function
    - System description
    - System name

  - System location
  - System contact
- IPv6 address
- IPv4 address
- MAC address including OUI
- MAC address (all-numeric)

Titles from the Prime configuration are inherited when you open your configuration. The only way to prevent the Prime title from being used is to assign a title yourself by using *Properties* on page 159. You cannot force the use of the default device title instead.

Effects

The **Find** dialog can search only on title preferences that are selected from this menu.

If Asset Tag is not selected, you cannot Find based on asset tag.

Limits

System description, system name, system location, system contact: Some values are treated as null—for example, Unnamed, Unknown, Unspecified, sysName. If a device has one of these names, the device title comes from the next available element. Network Discovery suppresses the value so that it can display another identifier that is more likely to help you recognize the device.

Default

Table 36: Device Title Preference defaults

Option	Example	Default	Source
Device-specific title	VOIP 6814 Dupont, Marie	ON	Device script
Domain name*	gateway.research.example.com	ON	DNS server
NetBIOS name* (network)	DUPONT	ON	Windows; SMB
NetBIOS name (scan)	DUPONT	ON	Scan file

* Requires that the device has an IP address.

Style Sheet

Allows you to designate a style sheet that customizes the look of Network Discovery. This custom style sheet augments the default Network Discovery style sheet; the custom style sheet does not replace the default.

Important: *for Netscape*—If you enter an invalid URL, Network Discovery may prevent you from accessing all pages that use style sheets. To recover from this, turn off style sheets in Netscape. (You may also need to quit Netscape.) Edit the URL to make it valid, then turn on style sheets in Netscape.

Effects

- Affects Device Manager, Port Manager, Line Manager, Attribute Manager, Service Analyzer, Home, Status, Reports, Administration and Help menus and pages.
- Does not affect map windows or the Health Panel.

Limits

Input

- must be a valid URL (for example, must begin with “http://”)
- *invalid characters:* space
- *length of input:* 0–256 characters

File

- must be a valid CSS level 1
- must be stored on a web server (not on the Peregrine appliance)

Technical

URL must be compliant RFC 2396.

Procedural alerts

Begin the URL with “http://”.

Automatic Packaging

Network Discovery can automatically package all similar end nodes into separate packages--all workstations in a workstation package, all printers in a printer package, and so on. Any end nodes not packaged in a separate package may still be put into a "catch-all" package. The "catch-all" package can contain any type of end node.

By default, Network Discovery automatically packages end nodes to reduce clutter and to focus attention on the more-important network connectivity devices.

You can change whether or not each class of end nodes is packaged, and whether packing priority is given to classes of end node, or whether all classes are treated as one.

Example 1

If you don't usually monitor end nodes, you might package all types of end node into a single type of package:

Set these controls **Off**:

- Workstations
- Servers
- Printers
- POS/ATM
- Controllers
- Unknown

Set this control **On**:

- End Nodes

Set the End Nodes threshold to **2**.

Example 2

If your network contains many servers for which you are responsible, you might package servers separately, but allow all other end nodes to be placed in a single type of package:

Set these controls **Off**:

- Workstations
- Printers
- POS/ATM
- Controllers
- Unknown

Set these controls **On**:

- Servers
- End Nodes

Set the Servers threshold to **1**.

Set the End Nodes threshold to **2**.

Example 3

If you are responsible for the three most common types of end nodes (workstations, servers, and printers), you might package each type separately for easy locating and identifying.

Set these controls **Off**:

- POS/ATM
- Controllers
- Unknown

Set these controls **On**, and set each threshold to **1**:

- Workstations
- Servers
- Printers
- End Nodes

End node packaging settings do not affect your ability to create custom packages.

The screen shows the current settings. The default is to package all classes, and to create the generic End Node class last.

Effects

Automatic packaging affects the map configurations of all accounts.

Limits

Automatic packaging settings do not affect your ability to create custom packages.

Default

By default, all package types are ON.

Table 37: Package class thresholds

Package class	Threshold
Workstations	3
Servers	3
Printers	3
POS/ATM*	3
Controllers	3
Unknown	3
End Nodes	2

* Point Of Sale / Automated Teller Machine

Procedural alerts

To collect all end nodes into a single class of package (to ignore end node types)

▶ Turn off all automatic package types except End Nodes.

NCDs with multiple end nodes will have a single package attached.

To have end nodes appear on the Main Map (never create any end node packages)

▶ Turn off all packages.

No end nodes will be packaged automatically.

Important: Turning off all packages is strongly discouraged. It causes map sessions to run slowly.

Element Management

You can access a separate management system through Network Discovery. You can launch an native application or a URL. The element manager can be launched on a specific device, either from a map window or from the Device Manager.

Network Discovery can automatically provide your element manager with the identity of the device—its IP address, MAC address, or DNS name. Where your element manager allows an identifier, include [IPv4] or [MAC] or [DNS] at the appropriate place in the path. Network Discovery automatically replaces [IPv4] or [MAC] or [DNS] with the address or name of the active device.

Example:

```
http://inventory.example.com/directory/devices.cgi?device=[IPv4]
```

Note: If you specify an IP address, and a device has only a MAC address and no IP address, you will be informed that the management could not be completed.

Effects

The name you enter appears in the **Object** menu of a map window. The name replaces *Manage* on page 157.

Options

- [IPv4]
- [MAC]
- [DNS]

Limits

Name

- valid characters: A–Z, a–z, 0-9, A–Z, a–z, 0–9, - *(hyphen)*, _ *(underscore)*, @ *(at sign)*, . *(period)*, *(space)*
- *length of input:* 0–20 characters
- names must be unique

URL or Native Application

- if URL, must be valid—that is, must begin with one of the following
  - http://
  - ftp://
  - nntp://
  - news:
  - gopher://
- *length of input:* 0–256 characters

Technical

URL must be compliant RFC 2396

Default

If a native application, and if no path is specified, the default operating system pathname is used.

Procedural alerts

- Begin a URL with “http://” (or other valid prefix).
- To have the names you choose appear in the **Object** menu of your map windows, you must click **Change** as usual, but you must also close and then re-open Health Panel and Network Map.

Tip: To reload the Toolbar, click one of the five left-most navigation links at the bottom of an Administration page or any similar page.

Note: *for Aggregator*—When viewing a remote appliance, the data for this page is supplied by the Aggregator appliance, not the remote appliance.

Related

- To manage a device from a map window, see *Manage* on page 157.
- To manage a device from the Device Manager, see *Manage* on page 199.

Device Manager Ports Display Preferences

- *List Preferences* on page 376
- *Reset to Defaults* on page 377
- *Add a Preference* on page 378
- *Preference Properties* on page 379
- *Delete a Preference* on page 379

The Device Manager has a Ports panel, which allows you to view the ports discovered for the device. Additionally, the Ports panel displays data for each port. You control the detail of the data displayed for each port within a display preference. Each preference appears in a pull-down list in the Ports panel. Each preference displays a table of data.

When defining a preference, you control how many columns each table has. You can have multiple display preferences. We supply you with two preferences to start.

List Preferences

Lists all Ports panel preferences. The list is sorted alphabetically by preference name.

The preference names are hyperlinked. Clicking the hyperlinks takes you to a shortcut menu where you are given the choice of modifying or deleting the preference.

Default

- status—a brief summary of the current state of the port
- details—a detailed overview of the port’s statistics

Reset to Defaults

Warning: You will delete all the Ports panel display preferences you have created. This action cannot be undone.

Deletes all added or modified preferences, and restores the default preferences:

- Status
  - Port Index (short)
  - Link Status
  - Details
  - Utilization State/In/Out
  - Errors Total
  - Connected to
- Details
  - Port Index (short)
  - Details (as a row)
  - Connected to (as a row)
  - Link Status
  - Breaks State
  - Utilization State/In/Out
  - Frames In/Out
  - Bytes In/Out
  - Unicasts In/Out
  - Broadcasts State/In/Out
  - Collisions State/Value
  - Errors State/In/Out
  - Delay State/Value

Notice that Port Index (short), Link Status, and Utilization State/In/Out appear in both defaults.

Add a Preference

Adds a Ports panel display preference. A preference must contain at least one element.

Table 38: Ports panel display preference options

Option	Default	Value	Limits
Name	—	valid characters	A–Z, a–z, 0–9, . *(period)*, - *(hyphen)*, _ *(underscore)*
	—	length of input (characters)	2–20
Description	same as Name	valid characters	*any*
		length of input (characters)	2–40
Element	Port Index	—	see Table 39

Table 39: Preference elements

Element	Description	Example
Port Index	The port index number and brief description of the interface.	2 / eth0
Port Index (short)	The port index number only (no description).	2
Interface Type	See *Interface Type [Administrator or IT Manager only]* on page 222.	Ethernet CSMA/CD
Interface Rate	See *Interface Rate [Administrator or IT Manager only]* on page 221.	10 Mbits/sec
Duplex	See *Duplex Mode [Administrator or IT Manager only]* on page 226.	Half
Details	The Interface Type, Interface Rate, and Duplex combined into a single column.	
Details (as a row)	The Interface Type, Interface Rate, Duplex, and Alarm Type as a separate row.	
Connected to	The connected device, the port number on the connected device plus short description, and a link of the Line Manager.	ws100-59.example.com (2 / Ethernet Port) [line]
Connected to (short)	The connected device, the port number on the connected device (no short description), and a link of the Line Manager.	ws100-59.example.com (2) [line]
Connected to (as a row)	The connected device, the port number on the connected device plus short description, and a link of the Line Manager—all in a row.	ws100-59.example.com (2 / Ethernet Port) [line]
Link Status	Signal light.	—
Breaks State	Signal light.	—
Utilization State/In/Out	Signal light and percentage value(s). Half-duplex ports have a single value; full-duplex ports have two values, one for incoming and one for outgoing.	
Frames In/Out	Frames/second for incoming and outgoing.	
Bytes In/Out	Bytes/second for incoming and outgoing.	
Unicasts In/Out	Unicasts/second for incoming and outgoing.	

Table 39: Preference elements (Continued)

Element	Description	Example
Broadcasts State/In/Out	Signal light and broadcasts/second for incoming and outgoing.	
Collisions State/Value	Signal light and collisions/second. Dependent on MIB.	
Errors State/In/Out	Signal light and error/second for incoming and outgoing. Dependant on MIB.	
Errors Total	Errors/second totalled for incoming and outgoing.	
Delay State/Value	Signal light and delays in milliseconds.	

Procedural alerts

- When using the list boxes, you can select multiple elements. *Windows users:* Hold down the Shift or Control key as you click the mouse.

Preference Properties

Modifies an existing Ports panel display preference. A preference must contain at least one element.

Table 40: Ports panel display preference options

Option	Default	Value	Limits
Description	same as Name	valid characters	*any*
		length of input (characters)	2–40
Element	Port Index	—	see Table 39 on page 378

Procedural alerts

- When using the list boxes, you can select multiple elements. *Windows users:* Hold down the Shift or Control key as you click the mouse.

Delete a Preference

Deletes a Ports panel display preference.

My Account Administration

My Account Administration is the same for Administrator accounts as it is for IT Employee and IT Manager accounts. For information, see *My Account Administration* on page 282 in *Chapter 19, Administration for IT Employee and IT Manager Accounts*.

My Map Configurations

My Map Configurations is the same for Administrator accounts as it is for IT Employee and IT Manager accounts. For information, see *My Map Configurations* on page 290 in *Chapter 19, Administration for IT Employee and IT Manager Accounts*.

21 CHAPTER How Network Discovery Works

You can use Network Discovery without ever having to read or refer to this section of the manual. However, experienced Network Discovery Administrators may find it easier to understand certain aspects of the behavior of Network Discovery after reading this section.

Exploration and Discovery

When you prepare Network Discovery for exploration, then set it going, Network Discovery begins by exploring the IPv4 ranges you have set up for discovery.

To begin with, this is strictly a yes-or-no proposition. The Network Explorer looks at each IP address and pings it to see whether or not there is a response. Is there a device at this address or not? The Network Explorer keeps running until it has made a sweep of all the address ranges that have been set up and has compiled a list of addresses where it got a positive response to its pings. The Explorer repeatedly recompiles this list to find any devices that have been added to the network. For faster rediscovery, the Explorer also tracks devices that respond positively and omits them the next time the list is recompiled.

As the list of devices is being compiled by the Network Explorer, the Network Interrogator requests as much of the list as has been completed. The Network Interrogator then attempts to identify each device in the list by using SNMP requests to read the device’s MIB. The Interrogator attempts to find out the device’s community strings, its domain name, NetBIOS name, how many ports each device has, and what type of device it is—whether it supports bridge tables, arp tables, Cisco CDP, source address capture, and so on. The result is called a device model.

Note: The Interrogator works on up to 250 device models concurrently.

The device model that the Interrogator develops is further refined by the Rulebase. This Rulebase takes the device model information and applies a set of “roles” to assigned icons, and priorities automatically. (You’ll find more information about the way an icon is assigned below—see *Icon assignment* on page 386.)

Once the Network Interrogator and Rulebase have identified the devices in the network, the Device Poller requests as many devices as have been identified. The Device Poller also read the device's MIB to get information about the device's traffic and connectivity on all of its ports. The Poller then passes its list of devices and ports to the Network Mapper.

Connectivity information also comes from the Table Reader. If the Interrogator has identified the device as a bridge, the Table Reader reads its bridge tables. If the device has been identified as a router, the Table Reader reads its ARP table.

The Network Mapper takes the list of devices and ports from the Realtime Poller and the information from the Table Reader. Using this data, the Mapper deduces what devices should be on the Network Map and how those devices should be connected.

The more data present, the more accurate Network Discovery is.

Once each of the processes described above has had a chance to run one time, it immediately starts all over again. The Network Explorer, Network Interrogator, Table Reader, Realtime Poller, and Network Map continue to run the entire time Network Discovery is in operation. In this way, Network Discovery constantly strives to present you with an updated view of your network, and constantly strives to improve the accuracy and depth of that view.

Table 1: RFCs and specifications supported by Network Discovery

RFC number	Name
RFC 1155	Structure and Identification of Management Information for TCP/IP-based Internets
RFC 1157	A Simple Network Management Protocol (SNMP)
RFC 1213	*see* RFC 2011, RFC 2012, RFC 2013
RFC 1285	FDDI MIB (SMT 6.2); *see also* RFC 1512
RFC 1315	*see* RFC 2115
RFC 1354	*see* RFC 2096
RFC 1398	*see* RFC 1643
RFC 1406	Definitions of Managed Objects for the DS1 and E1 Interface Types
RFC 1407	Definitions of Managed Objects for the DS3/E3 Interface Type
RFC 1493	Definitions of Managed Objects for Bridges (Bridge MIB)
RFC 1512	FDDI MIB (SMT 7.3)
RFC 1513	Token Ring Extensions to the Remote Network Monitoring MIB
RFC 1514	Host Resources MIB
RFC 1516	Definitions of Managed Objects for IEEE 802.3 Repeater Devices
RFC 1643	Definitions of Managed Objects for the Ethernet-Like Interface Types (Ethernet Interface MIB)
RFC 1695	Definitions of Managed Objects for ATM Management Version 8.0 using SMIv2 (ATM MIB)
—	ATM Forum 3.1 UNI specification
RFC 1748	IEEE 802.5 MIB using SMIv2

Table 1: RFCs and specifications supported by Network Discovery (Continued)

RFC number	Name
RFC 2011	SNMPv2 Management Information Base for the Internet Protocol using SMIv2
RFC 2012	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2
RFC 2013	SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2
RFC 2020	Definitions of Managed Objects for IEEE 802.12 Interfaces (100VG AnyLAN MIB)
RFC 2096	IP Forwarding Table MIB (Router MIB)
RFC 2115	Management Information Base for Frame Relay DTEs Using SMIv2 (Frame Relay MIB)
RFC 2233	Interfaces Group MIB using SMIv2
RFC 2668	Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)

Data from Express Inventory, the WMI collector

ServiceCenter's Express Inventory (WMI) collector gathers information about Windows workstations using Windows Management Instrumentation (WMI). This WMI information contributes to the Network Discovery database. References to scan files in the interface are to scan files that can be contributed by the Express Inventory (WMI) collector. For information on setting up and using the WMI Collector, see your ServiceCenter Essentials documentation.

ServiceCenter's Express Inventory (WMI) collector drops the XML scan files into a shared directory. Network Discovery accesses the files and presents the data:

- on the Network Map
- in Reports

The XML Enricher processes the XML scan files and passes information to the modeller. The remainder of the process continues as above except that scan-only devices are never polled.

Communication models

Frame relay

Network Discovery supports frame relay devices that conform to:

- RFC 2115, which supersedes RFC 1315

Each physical frame relay port may have one or more circuits associated with it. For some devices, Network Discovery is able to identify the circuits related to each physical port and gather traffic statistics both for the physical port and for each circuit. Network Discovery can also make connections between devices connected by these frame relay circuits.

The Device Manager Ports State panel presents the ports so as to make apparent the association between a physical port and its circuits. For devices on which Network Discovery is able to do a physical port mapping, each port is displayed in the form *x.y.z*, where *x* represents the slot or card number on which the port *y* is located, and *z* represents the frame relay circuit.

Using a Cisco 7200 router as an example, here's how Network Discovery arranges the port structure:

...	
1.5	—
1.6	—
1.7	frame relay physical port
1.7.27	frame relay circuit
1.7.32	frame relay circuit
2.1	—
2.2	—
...	

If a device supports frame relay but Network Discovery is not able to map the exact physical ports, each port is displayed in form *x.y*, where *x* represents the MIB-II object ifIndex and *y* represents to frame relay circuit. Using a Cisco 2500 router as an example:

1	—
2	—
3	—
4	frame relay physical port
4.75	frame relay circuit
4.76	frame relay circuit
4.78	frame relay circuit
5	—
6	frame real physical port
6.21	frame relay circuit
6.27	frame relay circuit

The line speed is set for each frame relay circuit. Each circuit should report a Committed Information Rate (CIR).

The CIR has meaning only for frame relay lines. It is used in service-level agreements and contracts for supply of communications bandwidth over frame relay lines. CIR has no functional impact on the performance of frame relay devices. For Network Discovery to read the CIR from the device, it must have been entered into the device's MIB. If Network Discovery cannot find the CIR in the MIB, it sets the frame relay circuit CIR to the line speed for that frame relay physical port.

If Network Discovery has determined the CIR incorrectly, you can use the Port Manager's *Interface Rate [Administrator or IT Manager only]* on page 221 button to redefine it. You may change the interface rate at either end or at both ends.

The following examples and rules describe the effect of setting the interface rate to set the CIR.

Suppose a frame relay line connects device A port 1 and device B port 2. The CIR (A1-B2) is defined from A1 to B2. The CIR (B2-A1) is defined from B2 to A1 and can have a different value from the CIR (A1-B2).

Table 2: Effects of setting CIR (example)

A1		B2		CIR A1 to B2	CIR B2 to A1
line speed (kb/sec.)	set by user	line speed (kb/sec.)	set by user	line speed (kb/sec.)	line speed (kb/sec.)
100	no	200	no	100	100
100	no	50	no	50	50
100	no	100	no	100	100
100	yes	50	no	100	50
100	yes	200	no	100	100
100	yes	50	yes	100	50
100	yes	200	yes	100	200

The rules that constructed this table are:

- The line speed is read from the device's MIB unless overridden by the user setting it.
- If the line speed is set by the user at one end, the CIR from this end is defined as that line speed.
- If the line speed is not set by the user at an end, the lower speed at either end defines the CIR for an end.

FDDI

Network Discovery has limited support for FDDI:

- support for the SMT v6.2 MIB (specified by RFC 1285)
- support for the SMT v7.3 MIB (specified by RFC 1512)

Network Discovery makes FDDI connections based on the MAC address and MIB variables for each device, not based on the FDDI port.

SMT (Station ManagementT) is an integral part of any FDDI implementation. SMT v6.2 can determine the upstream neighbor for an object. SMT v7.3 can determine both the upstream and downstream neighbors for an object.

Note: If you have a device that supports only SMT v6.2, check with the vendor or manufacturer for SMT v7.3 support. This will improve your FDDI connectivity.

Network Discovery uses the SMT instance—not the FDDI ports—when mapping FDDI objects. For example, if you have an FDDI concentrator with 8 ports, there is a single SMT instance, so Network Discovery shows only one uplink port and one downlink port for that concentrator.

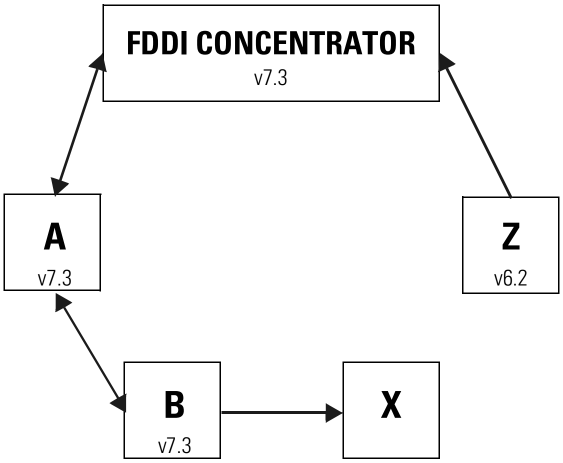
If Network Discovery cannot always close the logical ring for your network, it is because:

- all your FDDI objects have no SNMP management

- all your FDDI objects have SNMP management but support SMT implementations other than v7.3 or v6.2
- at any point in the ring, you have an FDDI object with no SNMP management immediately downstream of an object that supports only SMT v6.2.

To understand this last case, you must realize that the object with no SNMP management (X) is providing no “ring information” about itself to the FDDI ring.

Figure 21-1: FDDI ring that cannot be closed



The only way for the ring to remain unbroken is for the next object upstream (Z) to be able to look back downstream and ask object X about itself. If Z supports only SMT v6.2, then Z cannot see downstream, and therefore the ring cannot be closed.

If Network Discovery is ever unable to close the ring, check for objects with no SNMP management followed by an object with support for SMT v6.2 only. This is the only likely cause of a broken ring that will not be immediately obvious.

Icon assignment

Network Discovery assigns a device type to each device based on two factors: the Network Discovery Rulebase and the lexicographical analysis of the device’s MIB. The device type includes such characteristics as device icon, device description, device family, and device model.

For SNMP managed devices, both the Rulebase and lexicographical analysis of the MIB are used. For devices with no SNMP management, only the Rulebase is used. The device icon assigned to each of your devices is far more likely to be accurate if the device has SNMP management.

Reminder: If a device supports SNMP management, you should install or enable the SNMP agent for that device.

The Rulebase uses a device’s SysOID, SysDesc, and MAC address/OUI to implement rules that identify:

- Specific devices and device families. If a specific rule is not in the Rulebase, Peregrine Systems will add a rule for you, provided that:

    - your Peregrine appliance is under warranty
    - you can identify the devices by model or family (Peregrine would appreciate the URL for the manufacturer's web site whenever possible)

- you provide Peregrine with a CSV copy of your inventory containing the device.

- Probable device class (for devices and device families that do not match a specific identification rule). Such rules are likely to make good assignments for companies with small product lines and less accurate assignments for companies with large product lines. This is because these rules are based on:
    - advance classification of product lines; that is, some devices belonging to certain product lines can be identified by the beginning of the OUI
    - pre-identification of specific devices; that is, some devices can be identified because the manufacturers make only switches

Note: These rules may make incorrect assignments. You should contact Peregrine to request additional specific rules for devices if this happens.

- Specific operating systems.
- Specific (major) applications.

For devices with no SNMP management, the Rulebase can apply rules based only on information about the MAC address and OUI of the device. For each MAC address, the Rulebase identifies the most probable device class, based mostly on the OUI. (Very occasionally, manufacturers assign blocks of MAC addresses to specific products, which allows the Rulebase to make more specific identifications.)

The Rulebase also identifies the probability that each non-SNMP device may actually be an SNMP managed device providing network connectivity (such as a gateway, router, concentrator, or switch). SNMP managed devices can appear not to be managed when the device's IP address has been included in the list of Property Groups (see the *Setup Guide*) or when the community string for the device has not been included in the Network Discovery list of community strings (see the *Setup Guide*). In such a case, you should install or enable the SNMP agent for that device. (You may also need to modify the address scope or community strings.)

As with devices with SNMP management, class assignments for devices with no management work well for companies with small product lines and poorly for companies with large, varied products lines. Larger companies sometimes employ the same OUI for different products, but also use different OUIs for one product.

There is also a capacity to assign icons to unmanaged devices based on information contained in the NetBIOS and domain names has been added. For example:

- a device named "PRINTER3RDFLOOR" or "PRT3RDFLOOR" could be assigned a printer icon
- a device named "marysworkstation" could be assigned a workstation icon
- a device named "webserver.example.com" could be assigned a web server icon

Only the initial segment of the domain name is considered.

Domain and NetBIOS name interpretation is low priority. It never takes precedence in a situation where more accurate information is available. The rules used are not case sensitive.

Finally, Network Discovery can identify printers attached to printer servers. Many printer servers (both internal and external) do not provide enough information in their System Description to allow for accurate identification of the specific model of printer attached.

The Network Discovery Rulebase uses information that may be found elsewhere in the device MIB. For example, the System Description of this Hewlett-Packard printer server contains the following:

- HP ETHERNET MULTI-ENVIRONMENT,ROM H.08.01,JETDIRECT EX,JD34,EEPROM H.08.05

Note that this does not provide any information about the printer. The Enterprise MIB contains additional information that allows the Rulebase to identify the printer server as J3263A and the printer model as a HP LaserJet 5.

This capability can be expanded for types of devices other than printers and printer servers where information is available in portions of the MIB other than the System Description for more accurate identification.

Priority assignment

When the Rulebase assigns a device type, there is a priority associated with that type.

Table 3: Default device priority (sorted by priority)

Priority	Icon Name
4	100VG AnyLAN, Access Switch, ATM Switch, Backplane, Carrier Network, Cloud, Enterprise ATM, Enterprise Router, Enterprise Switch L2-, Enterprise Switch L3+, Ethernet/10, Ethernet/100, Ethernet/1000, FDDI, Firewall, Gateway, Local/Remote Access Server, Router, Switch L2-, Switch L3+, Token Ring, Transceiver, Unknown NCD, Unmanaged Hub, VPN Gateway, Wireless Access Point
3	Banyan Server, Mainframe/Large Server, Microsoft Server, NMS Appliance, Novell Server, Server, Storage Server, UNIX Server, Web Server
2	Analyser, Color Printer, Image Input, POS/ATM, Printer, Printer Server, Robot/Controller, UPS
1	Apple Workstation, Gadget, Laptop, Logical View, LV Unmapped, LV Unmapped IP, Microsoft Workstation, Network Computer, Shared Port, UNIX Workstation, Unknown, Unmapped IP, Workstation, X Terminal

Table 4: Default virtual device priority (sorted by priority)

Priority	Icon Name
4	Carrier Network, Cloud, Radio Cloud, Unmanaged Hub
1	Approximate, Logical View, LV Unmapped, LV Unmapped IP, Shared Port, Unmapped IP

Priorities 5 and 6 are reserved for the user to assign. By default, priority 6 is associated with those devices about which the user wishes to receive e-mail.

Presenting Information

As a user, you may find it easier to remember what conventions Network Discovery uses when displaying data if you understand a little about how Network Discovery operates.

Network Map

The Network Mapper has very little do with showing you the Network Map. The Network Mapper merely calculates the Network Map. The task of displaying the map is divided between two parts of a single process: map servers and the map client.

The map client—that is, the Network Map and other map windows—is the only part of the Network Discovery map system that you ever see.

When you click the **Network Map** button on the main Toolbar, Network Discovery performs three consecutive actions:

- begins a map session
- opens a map configuration
- opens a map window

These actions and concepts are separate, even though the actions are linked the first time they are performed. You will sometimes want to perform each action separately, so it helps to realize that each concept is distinct.

Map Session

The following session-based commands appear in the **File** menu:

- *Session Info* on page 136
- *Disconnect* on page 136
- *Reconnect* on page 137
- *Close Map* on page 138

When you begin a map session, you start receiving data from a Network Discovery map server. You continue to receive data from a Network Discovery map server until you exit the map session, or until you disconnect from the map session.

Each map session places demands on the resources of the Peregrine appliance. For this reason, the total number of map sessions per appliance is limited.

Each account is limited to a single map session per appliance. There are frequently more accounts than there are map sessions. You may be asked to leave your map session by another account who needs “map time”.

Administrator accounts can also disconnect an account from a map session.

Map Configuration

The following configuration-based commands appear in the **File** menu:

- *New* on page 131
- *Open…* on page 131

- *Open Copy of Prime* on page 131
- *Save* on page 132
- *Save As…* on page 132
- *Save As Prime [Administrator and IT Manager only] on page 133*

Any account can open or save a map configuration at any time during a map session. A map configuration file contains your settings for:

- layout, including the top object for each window
- packaging, including package icons
- object titles
- device priorities

You can use map configuration files to view the map from different perspectives. For example, one view might show the network by geography, while another might show the network logically, by subnet.

Network Discovery automatically opens a map configuration file at the start of each map session. The first time a new account starts a map session, the session always opens with a copy of the Prime configuration. All other times, the map configuration file that Network Discovery opens depends the type of account you are using.

Table 5: Default configuration files and accounts

Account type	Subsequent default file
Demo	Copy of Prime
IT Employee	last opened or designated
IT Manager	last opened or designated
Administrator	last opened or designated

When you end a map session, Network Discovery takes note of what map configuration file is in use. The next time you start a map session, Network Discovery opens that file. There are two exceptions:

- You can designate a different configuration file to be opened next time using the Administration menu. See *Manage Map Configurations* on page 290.
- Demo accounts always start a map session with a configuration called “Copy of Prime”. This is so that each user of a Demo account can start fresh, unaffected by other accounts.

  Demo accounts can open a saved configuration if they want to pick up where they left off.

If you end your session with “Copy of Prime”, you will get a fresh copy of Prime the next time you start a map session.

If you forget to save your map configuration before you end a map session, Network Discovery reminds you that your configuration has not been saved and offers you the chance to save it.

Each account has its own space for configuration files. You cannot overwrite or delete configurations belonging to others. For instance, you can have a configuration file named “test” and so can every other account—the files will not overwrite one another.

Loading and saving of map configuration files is disabled when using the **Forecast** command to view the Network Map.

Administrator and IT Manager: The Prime configuration is a special default configuration customized for use in your system. This configuration is customized and maintained by Administrator and IT Manager-level accounts.

Autosave

Configuration files are saved automatically every 2 minutes (or more frequently). This makes it possible for you to recover your configuration in the event of an abnormal occurrence, such as a power outage, or a disconnection from the map session or from the Peregrine appliance.

If a session ends abnormally, the recovery file will be opened the next time you start a map session, and you will be notified of the recovery with a dialog box: “Restored configuration from autosave”.

Even when Network Discovery loads the recovery file, you can still discard the recovery. Just re-open the configuration file that you last saved.

Note: Autosave never overwrites any configuration file that you have created. The autosave file is deleted any time you answer “No” to the question “Do you want to save the changes?”. The autosave file is also deleted every time you save a configuration.

Important: Always *Save* your map configuration before you *Close Map*. Do not rely on Network Discovery being able to recover the autosave file.

Prime configuration

The Prime configuration is a special configuration not associated with a particular account. Any Administrator or IT Manager account can overwrite the Prime configuration. To do so, see *Save As Prime [Administrator and IT Manager only] on page 133*.

The Prime configuration includes:

- packaging
- layout
- top objects
- icons (packages only)
- titles (all objects)
- priorities (devices)

Important: The Prime configuration in general—and its priorities in particular—control *Notification and Events Configuration* on page 328, the *Events Browser* on page 257, and most reports.

One Prime configuration setting cascades down to the configurations of other accounts:

- default titles (all devices)

This setting is used unless the owner of a configuration has changed the title of a device.

Table 6: Cascade of device titles from Prime configuration

Prime-assigned title	Account-assigned title	What the account owner sees
website	CorpWebSite	CorpWebSite
website	—	website

Device priority from the Prime configuration does not cascade to any other configurations. However, device priority does affect Notification and Events Configuration.

The default Prime configuration has end node packaging—all core devices are in the Network Map window. Layout, device priorities, and titles are all set to the default.

If you end your session with "Copy of Prime", you will get a fresh copy of Prime the next time you start a map session.

The Prime configuration is automatically updated every night just before Reports are generated. This ensures that the package names that appear in Reports match the Network Map.

Map Window

Window-based commands appear in the **File** menu:

- *Page Setup* on page 134
- *Print…* on page 135
- *Close* on page 138

Other window-based commands appear in the **View** menu:

- *Layout* on page 150
- *Underline Locked Objects* on page 152
- *Scale* on page 152
- *Scale Up* on page 153
- *Scale Down* on page 153
- *Fit Map to Window* on page 153
- *Fit Window to Map* on page 154

plus these packaging commands, which affect the layout:

- *Pack* on page 150
- *Unpack* on page 151
- *Unpack All* on page 151
- *Create Package* on page 152

(Packaging is also stored as part of the map configuration.)

Managers and reports

Network Discovery presents you with more information than is available from the Network Map. A good deal of this information is constantly collected at regular intervals, and is stored in Network Discovery databases.

The point is that Network Discovery does not use only the map client to present you with information. Information is presented using other interfaces and models.

Scheduled Events

The majority of data that Network Discovery uses is constantly being collected. However, some information is collected at a set time every day, while other information is summarized once a day.

This is a list of major events, not a complete list.

Table 7: Major events in the 24-hour timetable

Time	System event
0005–1900*	■ summarize statistics for each attribute† ■ perform internal backup to the Peregrine appliance’s internal hard disk drive† ■ perform external backup (if configured) to an FTP server and/or a tape drive† ■ update Prime configuration† ■ summarize events for reports† ■ compile and calculate reports†
0005–23:30‡	■ check devices for trashing and purging† ■ update list of exceptions†
0010	check evaluation license for expiry
0015	backup Prime configuration
0059	age out bridge tables of Plaintree WaveSwitch devices**

* If this series of events is not successfully completed, it will restart in 30 minutes and attempt to complete only the unsuccessful events from the series.
† Backups are performed only when the Peregrine appliance has been in operation for 2 hours.
‡ This series only begins once the previous series has finished.
** Is only done if you have provided a valid write community string for each device.

APPENDIX

A Need more help?

Peregrine is committed to ensuring your success with our products. We offer a number of ways for you to provide product feedback, suggest enhancements, and receive technical assistance with any issues you encounter.

For further information and assistance contact Peregrine's CenterPoint Web Site.

Peregrine's CenterPoint Web Site

Current details of local support offices are available through Peregrine's CenterPoint Web site at http://support.peregrine.com.

To find Peregrine worldwide contact information:

1 Log on with your login user name and password.

2 Click **Go** for **CenterPoint**.

3 Select **Whom Do I Call?** in the navigation bar on the left side of the page.

Peregrine worldwide information is displayed for all products.

APPENDIX B Copyright

Peregrine Systems acknowledges the copyrights belonging to the following third parties. (This page constitutes a continuation of the copyright page.)

JPEG Graphics Library

This software is based in part on the work of the Independent JPEG Group.

GD Graphics Library

Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, by Cold Spring Harbor Laboratory. Funded under Grant P41-RR02188 by the National Institutes of Health.

Portions copyright 1996, 1997, 1998, 1999, by Boutell.Com, Inc.

Portions relating to GD2 format copyright 1999 Philip Warner.

Portions relating to PNG copyright 1999, Greg Roelofs.

Portions relating to libttf copyright 1999, John Ellson (ellson@lucent.com).

Permission has been granted to copy and distribute gd in any context without fee, including a commercial application, provided that this notice is present in user-accessible supporting documentation.

This does not affect your ownership of the derived work itself, and the intent is to assure proper credit for the authors of gd, not to interfere with your productive use of gd. If you have questions, ask. "Derived works" includes all programs that utilize the library. Credit must be given in user-accessible documentation.

This software is provided "AS IS." The copyright holders disclaim all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation.

Although their code does not appear in gd 1.6.3, the authors wish to thank David Koblas, David Rowley, and Hutchison Avenue Software Corporation for their prior contributions.

GnuPlot Graphics Library

Copyright 1986–1993, 1998 Thomas Williams, Colin Kelley

Permission to use, copy, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation.

Permission to modify the software is granted, but not the right to distribute the complete modified source code. Modifications are to be distributed as patches to the released version. Permission to distribute binaries produced by compiling modified sources is granted, provided you

1. distribute the corresponding source modifications from the released version in the form of a patch file along with the binaries,
2. add special version identification to distinguish your version in addition to the base release version number,
3. provide your name and address as the primary contact for the support of your modified version, and
4. retain our contact information in regard to use of the base software.

Permission to distribute the released version of the source code along with corresponding source modifications in the form of a patch file is granted with same provisions 2 through 4 for binary distributions.

This software is provided “as is” without express or implied warranty to the extent permitted by applicable law.

Apache Webserver

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

PPP Server Software

Copyright © 1989 Carnegie Mellon University.

Copyright © 1991 Gregory M. Christy.

Copyright © 1993 The Australian National University.

Copyright © 1994 Philippe-Andre Prindeville.

Copyright © 1995 Eric Rosenquist, Strata Software Limited.

Copyright © 1995 Pedro Roque Marques

All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the Authors listed above. The names of the Authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

XNTP Network Time Synchronization

Copyright © David L. Mills 1992, 1993, 1994, 1995, 1996

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided “as is” without express or implied warranty.

SNMP Library/Server

Verification Utility

Strace Debugging Utility

File Identification Utility

lsof (List Open Files)

ICU Character Conversion Library

Glossary of Abbreviations

A—Ampere. Unit of electric current.

AC—Alternating Current. Electric current that reverses direction, as opposed to direct current, which always flows in the same direction. In most countries, the household electric current is AC.

ARP (pronounced "arp")—Address Resolution Protocol. ARP allows a device to find the physical address of a target device on the same physical network, given the IP address of the target device. An ARP request is broadcast to all devices on the same physical network, but only the target device replies with its IP address. Each device that uses ARP has an ARP cache of recently acquired IP-to-physical address bindings or pairings.

ATM—Asynchronous Transfer Mode. A networking technology with the capacity to transmit voice and video in real time as well as data, including frame relay traffic.

Note: ATM also stands for Automated Teller Machine. Network Discovery has a device icon dedicated to point-of-sale and automated tellers machines, POS/ATM.

CD—Compact Disc. A metal disc with a plastic coating. The disc is small enough to be held in the hand. A compact disc is used for storing digital data. Network Discovery software and licenses are supplied on compact discs.

CIDR— Classless Inter-Domain Routing. A format that allows you to abbreviate network mask (for example, 16) instead of typing it out (for example, 255.255.0.0). For further information, see *Netmask notation* on page 19.

CIR—Committed Information Rate. In a frame relay network, the bandwidth associated with a virtual circuit. The higher the CIR, the more priority given to the traffic for that circuit.

CPU—Central Processing Unit. A part of a computer that interprets and carries out instructions, usually a microprocessor chip.

CRC—Cyclic Redundancy Check, or Cyclic Redundancy Code. Cyclic redundancy checking is a method of examining data for errors by performing a computation on the data both before and after it is sent, and verifying that the computation yielded the same result each time.

CSV—Comma Separated Value. CSV files contain values from a spreadsheet, table, or database with each value separated by a comma. CSV files are extremely transportable—that is, they can easily be used by many kinds of software on many kinds of computers.

DC—Direct Current. Electric current that always flows in the same direction, as opposed to alternating current.

DHCP—Dynamic Host Configuration Protocol. DHCP assigns IP addresses to devices automatically, and can reassign them dynamically when there are more devices than there are IP addresses available. It also helps to manage IP addresses by having one location from which they are tracked and assigned.

DIN—Deutsche Industrie Norm. DIN is a German standards organization. A cable that has a DIN connector (for example, DIN-6) conforms to these standards.

DLCI—Data Link Connection Identifier. Part of the header in frame relay, the DLCI is used to route the frame.

DNS—Domain Name System. DNS is the system whereby domain names—such as "starter.example.com"—are first located (usually on a DNS server) and then translated into the less ambiguous but more difficult to remember IP addresses—such as "192.168.2.129". A DNS server is a computer that exists primarily to maintain a listing of which domain names correspond to which IP addresses. What this means to you is that you are allowed to work with and remember names, which are more likely to be meaningful than collections of numbers.

DTE—Data Terminal Equipment. Any device that can transmit digital information over a cable—for example, a microcomputer workstation. One of two types of computer hardware connected by an RS-232-C connection. The other type is DCE, or Data Communications Equipment—for example, a switch or modem.

ESD—ElectroStatic Discharge. The release of static electricity. Static electricity can damage or even destroy electronic equipment.

FAQ—Frequently Asked Questions—*see* **Knowledge Base**.

FCS—Frame Check Sequence. A method of checking the integrity of a frame. A FCS error indicates that the frame has somehow become corrupted, since the frame failed its CRC.

FDDI (sometimes pronounced "*fid*-dee")—Fiber Distributed Data Interface. FDDI is a set of rules for sending and receiving data on fiber optic lines to a local area network (LAN). FDDI is based on the token ring protocol, but uses two tokens instead of one. FDDI networks have a range of 124 miles / 200 km.

FS—File System. A file system is concerned with the naming and storing/retrieving of files, and comprises files (collections of data) and directories (collections of files).

FTP—File Transfer Protocol. FTP is a method for sending and receiving files from one place in a network to another.

HTML—HyperText Mark-up Language. HTML is a documentation standard intended to enhance the display of a document in a World Wide Web browser such as Netscape or Internet Explorer. For example, HTML codes for displaying subscript text (as in H_2O) look like this: "H<sub>2</sub>O"

HTTP—HyperText Transfer Protocol. HTTP is a method for exchanging files on the World Wide Web.

HSRP—Hot Standby Routing Protocol. A routing protocol that allows more than one router to act as a single virtual router. If one router fails, the next router assumes its identity immediately. As a result, as far as the rest of the network is concerned, the virtual router is still working.

Hz—Hertz. A unit of frequency of one cycle per second. This unit of measure is named for German physicist Heinrich Hertz.

ICMP—Internet Control Message Protocol. ICMP provides communication between the Internet Protocol (IP) software on one machine with the IP software on another. It is a simple protocol (or "set of rules and standards") that every IP-based device must support. ICMP is used to communicate control, information, and error messages among IP devices. Probably the best known ICMP messages are the echo request and echo reply messages of a ping.

IDE—Integrated Device Electronics. An interface for disk drives. Early Peregrine appliances used IDE drives. See also SCSI.

IE—Internet Explorer. Microsoft's Web browser software. Network Discovery is compatible with Internet Explorer and Netscape.

IP—Internet Protocol. The Internet Protocol (IP) handles the address part of each data packet that is transmitted from one computer to another on the Internet.

When you see the term "IP address" with no qualifiers in Network Discovery, it means that either a version 4 IP address (IPv4) or a version 6 IP address (IPv6) is acceptable.

- IPv4 address

An IPv4 address contains four sections separated by periods (or "dots"). Each section, called an octet, contains 8 bits expressed in decimal (0–255).

Example: 192.168.2.129

- IPv6 address

An IPv6 address contains eight sections separated by colons. Each section contains 16 bits expressed in hexadecimal (0000–FFFF).

Example: 1234:5678:9ABC:DEF0:1234:5678:9ABC:DEF0

Knowledge Base—The Knowledge Base at Peregrine Systems Customer Support has answers to questions customers have asked. It is available from the Help menu. The Knowledge Base covers topics best addressed in question-and-answer format rather than through conventional documentation, and acts as a catch-all place to describe quirks and common misunderstandings.

LAN (pronounced "lan")—Local Area Network. A LAN is a network of workstations sharing resources, usually within a restricted geographic area, such as an office building. LANs typically serve tens or hundreds of people rather than thousands. If your network has a single central site, you probably have a LAN. The main LAN technologies are Ethernet, token ring, and FDDI.

LED—Light Emitting Diode. A small light, sometimes round in shape. This term is also used for part of the Network Discovery user interface: a colored circle used to indicate alarm state—visible, for example, on the Health Panel.

LSN—Logical SubNet. A subnet (short for "sub-network") is a segment of a network. A logical subnet is a segment organized not by geography (where a device physically resides) but by netmask (short for "network mask").

MAC (pronounced "mac")—Media Access Control. A MAC address is a computer's unique hardware number. A MAC address looks like this—0040E5010025 —or like this—00 40 E5 01 00 25 (spaces added for readability). The six numbers are hexadecimal (base 16) values.

MB—MegaByte. A measurement of capacity, applied to such computer components as memory and disk storage.

MIB (pronounced "mib")—Management Information Base. A MIB is a collection of data that can be read and written using a network management protocol such as SNMP. The MIB is structured as a hierarchy of "objects". There are both standard MIBs (supported by many vendors) and proprietary MIBs (vendor-specific).

MTBF—Mean Time Between Failures. The average time that a device is operational. In Network Discovery, MTBF is measured in days. Devices that break frequently can cause you aggravation. In this context, the term refers to network devices such as switches and workstations, but both MTBF and MTTR could equally well refer to an automobile or telephone.

MTTR—Mean Time To Repair. The average time it takes to repair a device. In Network Discovery, MTTR is measured in hours. Devices that take a long time to repair can cause you considerable concern, particularly if they are important to the operation of your network.

NAT—Network Address Translation. NAT is an Internet standard that enables a local-area network to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. NAT servers have two main purposes: hiding private IP addresses from external addresses, and enabling a private network to use more private IP addresses.

NEWS—Network Early Warning System. This is the Network Discovery method of continually checking on the status of each individual device to see if it is likely to present you with problems in the near future. NEWS concentrates on devices likely to soon have an alarm (or warning) for packet loss or utilization, whichever will come first for that device.

NTP—Network Time Protocol. An Internet standard used to synchronize the clock of a computing device to a time server with a degree of accuracy of milliseconds. The Peregrine appliance can take advantage of NTP to set its internal clock accurately.

ODBC—Open Data Base Connectivity. An open standard for accessing a database.

OID—Object IDentifier. The number which identifies an object in a MIB. MIBs are made up of objects. Each object in a MIB has unique object ID, which is a series of numbers separated by dots. For example, the OID of system.sysName is ".1.3.6.1.2.1.1.5". This ID defines the location of that object within the MIB tree hierarchy.

OS—Operating System. A core computer program that manages all application programs. Often, OS is used as synonymous with DOS, or Disk Operating System.

OSI—Open Systems Interconnection. Usually in reference to the OSI network model. The OSI model has seven layers. Layers 2 and 3 are the most important to Network Discovery.

OUI (sometimes pronounced "*ow*-ee")—Organization Unique Identifier. The OUI is the first three octets of a MAC address, and it identifies the organization that manufactures the device associated with the MAC address. For example, in the MAC address "00 40 E5 01 00 25", the actual OUI is "00 40 E5". If the OUI is one that Network Discovery recognizes, then the first three numeric octets are replaced by either an abbreviation of the organization's name or the full organization name, depending on the context. For example, the Device Manager represents the MAC address "00 40 E5 01 00 25" as "PRGRIN 010025". Although Network Discovery has an extensive database of OUIs, there may be some it doesn't recognize, in which case all octets of the OUI are displayed numerically.

POS—Point of Sale. The point of sale is the place in a store where purchases are made. Point of sale devices include electronic cash registers and debit card readers.

PVC—Permanent Virtual Circuit. A logical (rather than physical) connection in a network, particularly in a frame relay network. With a PVC, you define connection points and let someone else worry about how the data physically moves from one point to the other.

RAM—Random Access Memory. Memory that can be used to store data. Different from ROM, read-only memory.

RH—Relative Humidity. The amount of water vapor actually in the air divided by the maximum amount of water vapor the air can hold at its current temperature.

RJ—Registered Jack. Modular wiring (receptacles and plugs) used to connect equipment over telephone lines. Examples are RJ-11 and RJ-45.

RS—Recommended Standard. The Electronic Industries Association has adopted such standards as RS-232 for serial communications.

SCSI—Small Computer System Interface. An interface for disk drives and other peripheral devices. Peregrine appliance use SCSI hard disk drives.

SMT—Station ManagemenT. This FDDI module operates at the data link and physical layers to monitor and manage both the FDDI ring and the devices on it.

SMTP—Simple Mail Transfer Protocol. SMTP is a set of rules concerning the sending and receiving of electronic mail (e-mail). An SMTP server is a device that exists primarily to perform the service of directing e-mail.

SNMP—Simple Network Management Protocol. SNMP is a set of rules that allow networks to be managed and devices on those network to be examined. This set of rules is a broadly accepted and implemented open standard. A device on which SNMP can perform actions (such as reading and writing the device's MIB) is said to be "managed". The chief benefit of SNMP is that it allows network managers to administer networks and devices remotely; that is, without having to physically locate and adjust each device.

Network Discovery uses SNMP to obtain information about your network and the devices within it. The SNMP standard allows Network Discovery to obtain this information in a manner that is independent of a specific network device implementation or its vendor.

TCP—Transmission Control Protocol. TCP is a communications protocol that sends data between network devices in the form of message units, or packets. TCP divides the data into packets at one end, and reassembles the packets once they arrive.

TCP/IP—Transmission Control Protocol/Internet Protocol. TCP/IP is the pairing of two protocols, TCP and IP. TCP/IP forms the basic communication language of the Internet. TCP/IP is not a program that you use; it is a pair of protocols required by programs that you use. For example, FTP, HTTP, SMTP, and Telnet use TCP/IP to make their connections.

U—Unit. Unit of measurement for rackmount equipment (U is 1.75in or 4.44cm)

UDP—User Datagram Protocol. An alternative communications protocol to TCP. Useful for network applications that have small data units to exchange.

UPS—Uninterruptible Power Supply. A piece of equipment that connects a device to a power source so that the principal source provides power when all is well, and the UPS's secondary source—a battery—provides power when the primary power source is not available, such as a blackout. Peregrine Systems strongly recommends the use of an uninterruptible power supply with the Peregrine appliance.

URL (sometimes pronounced "erl")—Uniform Resource Locator or Universal Resource Locator. The address of a file accessible through the World Wide Web. A URL looks like this: "http://www.example.com". Sometimes the "http://" is left off, and the URL is given simply in the form "www.example.com".

VA—Volt-Ampere. A measurement of power in an AC circuit.

VAC—Volts Alternating Current. Measurement of voltage swing.

VM—Virtual Machine. Any software that imitates the performance of a hardware device, such as a CPU.

WAN (pronounced "wan")—Wide Area Network. A WAN is essentially a network like a LAN, except with a broader structure and larger geographic area. If your network has a single central site, but also one or more remote sites (such as sales offices in other parts of the country), you probably have a WAN.

WWW—World Wide Web. If you create a file that can be transmitted using HyperText Transport Protocol (HTTP), and put it whether others can view it (by having their web browser temporarily transfer and display a copy of the file), then you are part of the World Wide Web.

Index

Peregrine
SYSTEMS®

April 16, 2003