

Peregrine

Network Discovery

User Guide

Copyright © 2002 Peregrine Systems, Inc. or its subsidiaries. All rights reserved.

Information contained in this document is proprietary to Peregrine Systems, Incorporated, and may be used or disclosed only with written permission from Peregrine Systems, Inc. This book, or any part thereof, may not be reproduced without the prior written permission of Peregrine Systems, Inc. This document refers to numerous products by their trade names. In most, if not all, cases these designations are claimed as Trademarks or Registered Trademarks by their respective companies.

Peregrine Systems® is a registered trademark of Peregrine Systems, Inc.

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 have comments or suggestions about this documentation, please send e-mail to Peregrine Systems Customer Support at support@peregrine.com.

This edition applies to version 5.0.1 of the licensed program.

Peregrine Systems, Inc.
Worldwide Corporate Campus and Executive Briefing Center
3611 Valley Centre Drive San Diego, CA 92130
Tel 800.638.5231 or 858.481.794-7428
Fax 858.481.1751
www.peregrine.com



Table of Contents

Chapter 1	Welcome to Peregrine’s Network Discovery	11
	How Network Discovery works	12
	Licensing explained	12
	Licenses by number of devices: an example	13
	Some information about Network Discovery evaluation periods	13
	Logging in to Network Discovery	13
	Shutdown and restart	15
	Shutting down the Peregrine appliance.	15
	Restarting the Peregrine appliance.	16
Chapter 2	Types of Account	17
	About accounts	18
	Demo accounts	18
	IT Employee accounts	19
	IT Manager accounts.	19
	Administrator accounts	20
Chapter 3	Setting up Accounts	23
	Generating a list of accounts	24
	Adding an account.	24
	Customizing an account’s properties.	26
	Modifying account contact information	30
	Modifying an account password.	31
	Deleting an account	32

Chapter 4	Maintaining Your Account	35
	Customizing your account	36
	Modifying your contact data	39
	Modifying your password	40
	Testing your e-mail address.	41
	Testing your pager address	42
	Testing your pager number	42
Chapter 5	A Tour: Toolbar, Health Panel, Network Map	45
	The Toolbar is the starting point	46
	Navigating with buttons and links	47
	See an overview with the Health Panel	48
	You can minimize the Health Panel	48
	Report buttons on the Health Panel show overall performance.	49
	Buttons for the performance of Network Discovery	49
	The Network Map provides a graphical view	51
	Status Bar	53
	What are the icons on the map?	54
	Device icons	55
	Package icons group other icons together.	55
	Virtual device icons show that connectivity is not clear	56
	Other Icons	59
	The behavior of “scanned-only” devices	61
Chapter 6	A Tour: Managers, Events Browser, Service Analyzer, Reports	63
	The Device Manager	64
	The Port Manager	66
	The Attribute Manager	66
	The Line Manager	67
	The Events Browser	70
	The Service Analyzer.	72
	Find	75
	Administration	78
	Reports.	78
	Executive Summary/Network Reports	78
	WAN Reports	79

	LAN Reports	79
	Device Reports	80
	Support Reports	80
	You can use Network Discovery data with other applications	80
	Status	81
Chapter 7	Customizing Your View of the Network Map 83	
	Customizing for any accounts.	84
	Renaming an object	84
	Customizing how you see the map.	84
	Customizing alarm and warning colors.	88
	Placing an object at the top of the map window	89
	Changing the priority of a device	90
	Customizing for IT Manager and Administrator accounts	91
	Changing a device icon	91
	Customizing map contents	93
	Changing Alarm Thresholds	96
Chapter 8	Packaging Your Network	101
	How packaging works	102
	Network Discovery creates end node packages automatically	103
	You can request the creation of packages	104
	You can create your own multi-object packages	105
	Locked objects	106
	Changing the automatic packaging preferences	107
	Changing a package icon	108
Chapter 9	Organizing Map Configuration Files	109
	The Prime configuration	110
	Saving your changes	110
	Starting a map configuration	111
	Saving a map configuration file	111
	Saving the Prime map configuration	112
	Opening a saved map configuration file	112
	Managing map configuration files	113

	Sharing map configuration files with other accounts	114
	Restoring the Prime map configuration	115
Chapter 10	Setting up Paging	117
	Tasks <i>not</i> covered in this chapter	118
	Installing and setting up an external modem or an SMTP server	118
	Entering the e-mail address.	118
	Setting up event filters	119
	Adding a new service provider	119
	Listing your service providers.	120
	Testing your pager service provider	121
	Modifying modem properties.	122
	Modifying account profiles	123
	Configuring event filters for paging	124
	Testing the pager address.	124
	Testing the pager number	125
	Modifying information for a service provider	125
	Deleting a service provider	127
Chapter 11	Setting up Event Filters	129
	Interactions that affect Event Filters	130
	What is an Event Filter?	131
	Preparing Network Discovery for Event Filters	132
	Examples of common Event Filters	133
	Example 1: Notification when a core device breaks	133
	Example 2: Notification when a router is dropping a lot of traffic.	135
	Example 3: Notify me when a line to an important device has long delays	137
	Modifying a filter	140
	Deleting a filter	142
	Listing Event Filters	142
	Resetting to Defaults.	143
Chapter 12	Locating Network Problems	145
	Finding the problem by means of the Service Analyzer	146
	Once you have found the problem.	146
	Using the Network Map and the managers	147

	Start with the Network Map and Health Panel	148
	Using the Health Panel Reports	148
	Checking network events with the Events Browser	149
	Drill down with the Device Manager	150
	Device Manager panels	150
	Checking a device with the Device Manager	152
	Drill down with the Line Manager	153
	Drill down with the Port Manager	153
	Port Manager panels	154
	Check ports with the Port Manager	155
	The Attribute Manager	155
	Sample troubleshooting scenarios	156
	Example 1: Device Break	156
	Example 2: Collision	158
Chapter 13	Adding, Removing, and Replacing Devices	159
	The importance of unique IP addresses	160
	Removing a device	160
	Adding a device	161
	With a new IP address	161
	With the same IP Address as a trashed device	161
	Replacing a device	162
	With an identical device	162
	With a different device.	162
	Changing the IP address of a device	163
	Changing the cards or ports in a device	163
	Resetting the MTTR and MTBF	164
Chapter 14	Deleting Data, Connections, and Devices	167
	Deleting data	168
	Deleting connections	169
	Changing the device trash and purge (expiry) intervals	170
	Changing the device purge intervals	171
Chapter 15	Connecting with Another Management System	173
	Connecting from Network Discovery to another system	174

	Setting up the default URL or application.	174
	Opening the other system	175
	Connecting to Network Discovery from another system	175
	Device Manager	176
	Port Manager	177
	Line Manager	178
	Attribute Manager	179
	Service Analyzer	182
	Other components	182
Chapter 16	Vacations and Weekends	185
	Before you go away	186
	Set the Trash and Purge intervals	186
	Change who will be notified when events occur	186
	When you come back	187
	Top priority	187
	Second priority.	188
	Third priority	188
	Checking individual devices	188
Chapter 17	Using an Aggregator	189
	What's an Aggregator?	190
	How do I use the Aggregator?	190
	Installing your Aggregator license	191
	The Aggregator Toolbar	191
	Setting up the Aggregator and remote appliances to work together	192
	Setting up the remote appliances for access	193
	Navigating through multiple appliances	195
	Using the pull-down list on the Toolbar	196
	Using the Remote Appliances list	196
	The difference between Home and Home Base	197
	Using the Aggregate Health Panel	199
	Appliances button	200
	Exceptions button	201
	The Aggregate Events Browser	201

Chapter 18	Using Proxy Services	203
	Four examples	204
	Using the default—no proxy	204
	Description	204
	How to set it up	205
	Proxy access through a remote appliance	206
	Description	206
	How to set it up	206
	Proxy access through the Aggregator	207
	Description	207
	How to set it up	208
	Proxy access through the Aggregator and remote appliances	209
	Description	209
	How to set it up	210
	Index	211

1 | Welcome to Peregrine's Network

CHAPTER | Discovery

This *User Guide* is for anyone who will use Network Discovery, regardless of the level of access (type of account). It explains how to use the Network Discovery software—including the Health Panel, the Network Map, the Events Browser, the Device Manger and Service Analyzer—to manage your network.

Topics in this chapter, include:

- *How Network Discovery works* on page 12
- *Licensing explained* on page 12
- *Logging in to Network Discovery* on page 13
- *Shutdown and restart* on page 15

How Network Discovery works

A more detailed explanation is available in the *Reference Manual*.

Network Discovery pings and polls its way through your network to arrive at an understanding of the network's physical topology. It uses SNMP information—ARP caches, bridge tables, source address capture and port-by-port traffic analysis. Typically, this process adds 2% or less overhead to the 10 Mbps Ethernet segment that the Network Discovery is directly connected to, though it can add up to a maximum of 5% on some networks (0.5%, if the Ethernet segment is 100 Mbps). The overhead decreases farther away from the Network Discovery segment, diminishing through core switches and out through edge routers.

Network Discovery provides a real-time view of the network and its relationships, allowing you to understand the network as it fits into the overall infrastructure and to monitor changes in the network's assets over time. You have the tools to view, analyze, and report on your network.

Licensing explained

The Network Discovery licensing system allows many options to suit customer needs.

Licenses are based on:

- how many devices are in the network
- whether or not you have an Aggregator (a license that lets you link Peregrine appliances)
- Whether or not you are evaluating the Peregrine appliance
 - How long the evaluation period is
- The length of the maintenance / warranty period

Note: Features that are unavailable with your license are gray in the interface or are not visible at all.

Note: You can find information about what license has been purchased and installed on your Peregrine appliance at **Status > Current settings > Installed Licenses**.

Licenses by number of devices: an example

If you order a license for 1,000 devices, your license will handle six times as many ports as devices (6,000). The maximum number of ports is 45,000, regardless of the number of devices.

Some information about Network Discovery evaluation periods

The evaluation period gives you time to try out Network Discovery with your system before purchasing it.

- The evaluation period begins as soon as Network Discovery discovers something and adds it to the database.
- At the end of the evaluation, the appliance still functions, but access to the Map and Toolbar shuts off, so Network Discovery is unusable.

There are three ways to extend the time:

- Receive an extension license
- Clear the database
- Buy the product. You will receive a new license.

Logging in to Network Discovery

This login procedure works for any Network Discovery product.

To log in to the Peregrine appliance:

- 1 Launch your web browser.
- 2 In the URL area of the browser, enter the IP address or domain name of your Network Discovery appliance.

When the connection is made, the Network Discovery splash screen appears, followed by the Login window.

Note: To make the Login window appear sooner, click the Network Discovery splash screen. You can bookmark this URL for use with your browser.

Figure 1-1: Network Discovery splash screen

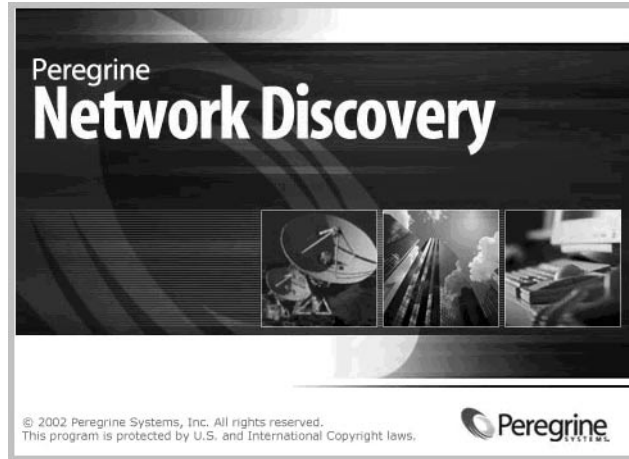
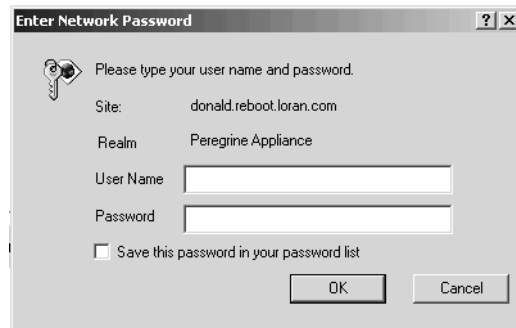


Figure 1-2: Network Discovery login window



- 3 Enter your account name (user name) and password.

If your Network Discovery Administrator has not supplied you with an account and password, use the account name “demo” and the password “demo”.

Important: Account names are all lower case. Passwords are case-sensitive. “DEMO” and “demo” are two different passwords.

Note: If you are the Network Discovery Administrator and you want information on setting up accounts with user names and passwords, see *Setting up Accounts* on page 23.

Once the user name and password are accepted, the Network Discovery home page and Toolbar appear. You may have a short wait while the Toolbar loads. If you have any problems logging in, see the *Network Discovery Setup Guide*.

Figure 1-3: Network Discovery Toolbar



Shutdown and restart

Warning: It is extremely important to shut down the Peregrine appliance properly. If the correct shutdown procedure is not followed, you risk corrupting the Peregrine appliance. Make sure that every person who may come into contact with the Peregrine appliance understands how to shut it down properly.

Shutting down the Peregrine appliance

Appliance Shutdown lets you shut down the Peregrine appliance safely. 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 the hard drive. Whenever possible, the Peregrine appliance should be powered off in an orderly fashion.

To shut down the Peregrine appliance

- 1 Click **Administration > Appliance management > Appliance shutdown**.
- 2 Click **Shut down appliance**.
- 3 Wait at least 2 minutes.

Warning: You can damage the Peregrine appliance hard drive if you do not wait at least 2 minutes for activity to stop. Do not turn the appliance off, if a flashing light indicates that it is still active.

You will not see any indication of the progress or successful completion of the shutdown. You must wait at least 2 minutes.

- 4 Turn the power switch to the off position. (On the IBM xSeries e-server, manually press the power-control button.)

Restarting the Peregrine appliance

Appliance Restart will restart the Peregrine appliance safely. You would use this procedure in the following situations:

- You are upgrading the Network Discovery software.
- Peregrine Systems Customer Support has suggested you restart the Peregrine appliance.

To restart the Peregrine appliance

- 1 Click **Administration > Appliance management > Appliance restart**.
- 2 Click **Restart appliance**.
A message asks you to wait.
- 3 Wait 8–9 minutes.

2 Types of Account

CHAPTER

All Network Discovery system configurations can support up to 250 accounts (including at least one Administrator account).

Topics in this chapter include:

- *About accounts* on page 18
- *Demo accounts* on page 18
- *IT Employee accounts* on page 19
- *IT Manager accounts* on page 19
- *Administrator accounts* on page 20

About accounts

There are four types of account:

- Demo
- IT Employee
- IT Manager
- Administrator

The Peregrine appliance is always shipped 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 will see how many of the map sessions are currently available.

Demo accounts

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.

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.

A Demo account can:

- View the Network Map, with the restriction that each map session will begin with a configuration named “Copy of Prime.” The Prime configuration is maintained by an Administrator or IT Manager account.
- Open any saved map configuration
- Save any number of map configurations

IT Employee accounts

An Administrator account owner can create (or delete) all account names and passwords, but IT Employee and IT Manager account owners can change their own passwords.

An IT Employee account can:

- Do everything a Demo account can do
- View the Network Map; with every map session after the first session automatically loading their default configuration (which is normally the configuration used most recently)
- Manage their own configurations (delete, duplicate, and rename them, and set a default configuration without opening the Network Map)
- Change their own password and account profile

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.

An IT Manager account can:

- Do everything an IT Employee account can do
- Set appliance system variables such as system name, system contact, system location
- Save a copy of the Network Map as prime

- See a device's read and write community strings (if known) in the Device Manager Configuration panel
- Purge a device, port or attribute from the Network Map
- Change a device icon
- Reset the Mean Time To Repair (MTTR) and Mean Time Between Failures (MTBF) for a device
- Update the model for a device
- Change how Network Discovery sees connections between objects, and break existing connections and create custom connections
- Set SNMP variables in the MIB Browser

Administrator accounts

Warning: 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.

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.

An Administrator account can:

- do everything that IT Manager accounts can do
- perform initial configuration of the Peregrine appliance
- configure the Peregrine appliance operations on the network
- administer the IT Manager, IT Employee and Demo accounts
- set SNMP variables in the MIB Browser

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 Customer Support.

Table 2-2: What the accounts can do

	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	—	—	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 <i>set</i> 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

	Demo	IT Employee	IT Manager	Administrator
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				
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

3 Setting up Accounts

CHAPTER

This section is for the Network Discovery Administrator only.

All of these commands are available when you click Administration > Account administration.

These procedures allow you to create, delete, and configure user accounts.

Topics in this chapter include:

- *Generating a list of accounts* on page 24
- *Adding an account* on page 24
- *Customizing an account's properties* on page 26
- *Modifying account contact information* on page 30
- *Modifying an account password* on page 31
- *Deleting an account* on page 32

Generating a list of accounts

This page provides an alphabetical list of currently registered users, complete with their full name and e-mail address. The user names in the list are hyperlinked, so that you can click on the name and see all the options you can perform on that account.

To generate a list of all accounts

- ▶ Click **Administration > Account administration > List accounts**.

A list of all the accounts appears. To modify an account, you can click on the Account name, or go back up a level to the **Account Administration** page and click **Account properties**.

Figure 3-1: List of accounts

Account Name	Account Type	Name	E-mail Address
admin	Administrator	Administrator	n/a
demo	Demo	Demo Account	n/a
itemployee	IT Employee	IT Employee	n/a
itmanager	IT Manager	IT Manager	n/a

Adding an account

There can be as many as 250 accounts, including yours.

Warning: 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.

The account name must be 3–20 characters long. Acceptable characters are:

- a through z
- 0 through 9
- underscore (_) (the underscore cannot be the first character in the account name)

Note: Uppercase letters are not acceptable.

To add an account

- 1 Click **Administration > Account administration > Add an account.**

Enter a login name. Acceptable characters are:

- a through z
- 0 through 9
- underscore (_) (the underscore cannot be the first character in the account name)

- 2 Click **Add Account.**

Note: The account is created, but you must still create a password for the account. If you do not create a password, no one will not be able to log in with it.

Figure 3-2: Add an account



Account name:
user_account

Add Account

Customizing an account's properties

You can change the level of access, access to various Network Discovery capabilities and any of the account properties listed in the following table:

Table 3-1: 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
<ul style="list-style-type: none"> ■ Web Access 	<ul style="list-style-type: none"> ■ 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).
<ul style="list-style-type: none"> ■ MySQL ODBC Access 	<ul style="list-style-type: none"> ■ allows owner of the account to export Network Discovery data to third-party data access applications to create custom reports.
<ul style="list-style-type: none"> ■ Shared directory Access 	<ul style="list-style-type: none"> ■ the shared directory is for downloading license files and Express Inventory, the WMI collector scan files
<ul style="list-style-type: none"> ■ SMB share 	<ul style="list-style-type: none"> ■ for depositing Express Inventory, the WMI collector scan files
Name	The name of the account owner.
Allow others to copy map configurations	Determines whether or not other users can copy map configuration files from this account.
Receive a copy of Network Discovery status reports by e-mail	Determines if the account owner will receive status reports from Network Discovery.
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.

Property	Explanation
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	Applies to Device Manager, Port Manager, Line Manager, Attribute Manager and Service Analyzer
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 will 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 will appear initially when you open a Device Manager session.
Default Port Manager panel	Determines which panel you will see first when you open a Port Manager session.
Default Find panel	Determines which panel you will see first when you open a Find session.
Default Attribute panel	Determines which panel you will see first when you open an Attribute Manager session.
Default Device Manager Ports panel selection	Determines which panel you will see first when you open a Ports session from the Device Manager.
<ul style="list-style-type: none"> ■ increment 	<ul style="list-style-type: none"> ■ Determines how many rows of data the Ports panel displays at a time. Default: 24
Default Events Browser selection	Determines which panel you will see first when you open an Events Browser session. You can see all of the events or choose one.
<ul style="list-style-type: none"> ■ increment 	<ul style="list-style-type: none"> ■ Determines how many rows of data the Events Browser displays at a time. Default: 20

To select an account for customizing

- 1 Click **Administration > Account administration > Account properties**.
- 2 Select an account from the list box.
- 3 Click **Modify Properties**.

To modify an account

- 1 Select an account type from the list box.

Note: You cannot change the account type for the account you are currently using.

- 2 Determine what capabilities the account will have.

Note: You cannot change the web access capability for the account you are currently using.

- 3 (*optional*) Enter a descriptive name in the Name field.

- 4 Assign the appropriate properties.

5 Click Modify Properties.

Figure 3-3: Modify account properties

Account type:	<input type="text" value="IT Employee"/>
Account capabilities:	Web Access: <input checked="" type="radio"/> Yes <input type="radio"/> No MySQL ODBC Access: <input type="radio"/> Yes <input checked="" type="radio"/> No ApE Access: No (no licence) Shared directory Access: <input type="radio"/> Yes <input checked="" type="radio"/> No
Name:	<input type="text"/>
Allow others to copy map configurations?	<input type="radio"/> Yes <input checked="" type="radio"/> No
<hr/>	
Append IP Address to device titles?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Make URLs visible?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Draw borders on tables in text mode?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Alternate colors in table rows?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Highlight table rows on mouse over?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Show navigation bar?	<input checked="" type="radio"/> Yes <input type="radio"/> No
<hr/>	
Time before marking statistic as stale:	Days: <input type="text" value="0"/> Hours: <input type="text" value="2"/> Minutes: <input type="text" value="0"/> Seconds: <input type="text" value="0"/>
Long date format: [Help]	<input type="text"/> default: %A, %B %e, %Y %T %Z
Short date format: [Help]	<input type="text"/> default: %Y-%m-%d %R
<hr/>	
Inline help format:	<input type="text" value="All"/>
<hr/>	
Default Device Manager panel:	<input type="text" value="State"/>
Default Port Manager panel:	<input type="text" value="State"/>
Default Find panel:	<input type="text" value="Device"/>
Default Attribute panel:	<input type="text" value="Configuration"/>
Default Device Manager ports panel selection:	<input type="text" value="Status"/> increment: <input type="text" value="10"/>
Default Events browser selection:	<input type="text" value="All"/> increment: <input type="text" value="10"/>
<hr/>	
<input type="button" value="Modify Properties"/>	

Modifying account contact information

You can change any of the following properties:

- E-mail address (optional, but required if the user is to receive any e-mail about the Peregrine appliance or the network)
- Pager e-mail address
- Pager number
- Pager service provider

To modify an account's contact information

- 1 Click **Administration > Account administration > Account contact data**.
- 2 Select an account name from the pull-down list.
- 3 Click **Modify Properties**.
- 4 You can now modify any of the contact information.
- 5 Check to make sure the changes are correct.
- 6 Click **Modify Contact Data**.

To enable e-mail notification

- ▶ Enter an e-mail address in the E-mail address field.
If the e-mail address is blank, the user will not receive any e-mail, even when the receive list box is set to "yes".

To enable pager notification through an e-mail gateway

- ▶ Enter a pager address in the Pager e-mail address field.

To enable direct alphanumeric pager notification

- 1 Enter a pager number.
- 2 Select a pager service provider from the list box.

Note: The list of pager service providers must be created by an Administrator account. See *Setting up Paging* on page 117.

Figure 3-4: Modify contact data

The screenshot shows a web form titled 'Modify Contact Data'. It has the following fields:

- E-mail address:**
- Pager e-mail address:**
- Pager number:**
- Pager Service Provider:** (dropdown menu)

At the bottom left of the form is a button labeled 'Modify Contact Data'.

Modifying an account password

An Administrator account must create an account password while creating a new account, or can modify the password at any other time.

Passwords can be up to 20 characters long. Acceptable characters are:

- A through Z
- a through z
- 0 through 9
- underscore (_)
- at (@)
- period (.)
- hyphen (-)

To modify an account password

- ▶ Click **Administration > Account administration > Account password**.

To select an account


- 1 Select an account from the list box.
- 2 Click **Modify Account**.

To modify or create a password

- 1 Enter the new password in the first field.

- Do not enter the current password (if any).
- 2 Enter the same new password in the second field.
Entering the same password twice helps guard against typing errors.
 - 3 Click **Modify Password**.

Figure 3-5: Modify password



The screenshot shows a web form for modifying a password. It contains two text input fields. The first field is labeled "Password:" and contains a masked password represented by asterisks. The second field is labeled "Password (again):" and also contains a masked password. Below the input fields is a button labeled "Modify Password".

Deleting an account

This page allows the Administrator account to delete an account from the list of current accounts.

Note: The account you are using to delete accounts, or the “active” account, cannot be deleted.

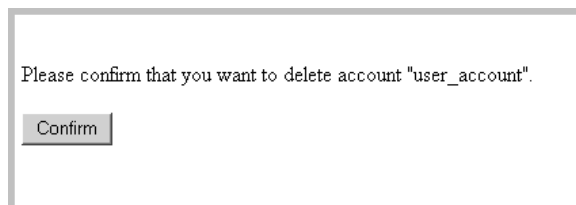
To select an account

- 1 Click **Administration > Account administration > Delete an account**.
- 2 Select an account from the list box.
- 3 Click **Delete Account**.

To delete an account

- ▶ Click **Confirm**.

Figure 3-6: Delete an account



Troubleshooting

Why do I see “Account name ‘delme’ does not exist.” when I try to delete an account?

Two possibilities:

- Another Administrator account deleted the account just before you did.
- You deleted the account yourself, but the account login name still appears in the list box because the list has not been updated. To get an updated list of accounts, click your web browser’s Reload or Refresh button.

4 Maintaining Your Account

CHAPTER

This section is intended for Administrator, IT Manager, and IT Employee accounts.

The Demo account cannot perform any administration functions.

You can maintain your own account by setting your own preferences, contact information, and even your password. An Administrator account can also do these tasks as part of setting up accounts.

Topics in this chapter include:

- *Customizing your account* on page 36
- *Modifying your contact data* on page 39
- *Modifying your password* on page 40
- *Testing your e-mail address* on page 41
- *Testing your pager address* on page 42
- *Testing your pager number* on page 42

Customizing your account

The Network Discovery Administrator (with an Administrator account) sets up your account and determines what levels of access and capabilities you will have, but you (as the user of an IT Employee, IT Manager or Administrator account) can customize your own preferences.

You can change any of the account properties listed in the following table.

Note: Many of these properties will be of more interest to you when you are more experienced with Network Discovery. There is more information on them in the *Reference Manual*.

Table 4-1: Account properties that IT Employee, IT Manager, and Administrator accounts control

Property	Explanation
Name	The name of the account owner.
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 more space on your screen.
Alternate colors in table rows	Tables are easier to read with alternating colors, but they take up 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	Applies to Device Manager, Port Manager, Line Manager, Attribute Manager and Service Analyzer
Long date format	Determines how the date is displayed at the bottom of most panels and pages.

Property	Explanation
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 will 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 will appear initially when you open a Device Manager session.
Default Port Manager panel	Determines which panel you will see first when you open a Port Manager session.
Default Find panel	Determines which panel you will see first when you open a Find session.
Default Attribute panel	Determines which panel you will see first when you open an Attribute Manager session.
Default Device Manager Ports panel	Determines which panel you will see first when you open a Device Manager Ports panel:
Default Events Browser	Determines which panel you will see first when you open a Port Manager session.

To customize the properties of your account

- 1 Click **Administration > My account administration > Account properties**.
A screen appears called "Account Properties for [account name]".
Note: If no password is given, the account cannot be used to log in, even when Web Access is set to "yes".
- 2 Choose the properties you want.

3 Click Modify Properties.

Figure 4-1: Modify account properties

Account type:	IT Employee		
Account capabilities:	Web Access:	Yes	
	MySQL ODBC Access:	No	
	ApE Access:	None	
	Shared directory Access:	No	
Name:	<input type="text"/>		
Allow others to copy map configurations?	<input type="radio"/> Yes <input checked="" type="radio"/> No		
<hr/>			
Append IP Address to device titles?	<input type="radio"/> Yes <input checked="" type="radio"/> No		
Make URLs visible?	<input type="radio"/> Yes <input checked="" type="radio"/> No		
Draw borders on tables in text mode?	<input type="radio"/> Yes <input checked="" type="radio"/> No		
Alternate colors in table rows?	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Highlight table rows on mouse over?	<input type="radio"/> Yes <input checked="" type="radio"/> No		
Show navigation bar?	<input checked="" type="radio"/> Yes <input type="radio"/> No		
<hr/>			
Time before marking statistic as stale:	Days:	<input type="text" value="0"/>	Hours: <input type="text" value="2"/> Minutes: <input type="text" value="0"/> Seconds: <input type="text" value="0"/>
Long date format: [Help]	<input type="text"/> default: %A, %B %e, %Y %T %Z		
Short date format: [Help]	<input type="text"/> default: %Y-%m-%d %R		
<hr/>			
Inline help format:	<input type="text" value="All"/> <input type="button" value="v"/>		
<hr/>			
Default Device Manager panel:	<input type="text" value="State"/> <input type="button" value="v"/>		
Default Port Manager panel:	<input type="text" value="State"/> <input type="button" value="v"/>		
Default Find panel:	<input type="text" value="Device"/> <input type="button" value="v"/>		
Default Attribute panel:	<input type="text" value="Configuration"/> <input type="button" value="v"/>		
Default Device Manager ports panel selection:	<input type="text" value="Status"/> <input type="button" value="v"/>	increment:	<input type="text" value="10"/>
Default Events browser selection:	<input type="text" value="All"/> <input type="button" value="v"/>	increment:	<input type="text" value="10"/>
<hr/>			
<input type="button" value="Modify Properties"/>			

Modifying your contact data

Network Discovery can communicate with you by e-mail or pager to do such things as inform you that an important device is broken or let you know whether a backup of Network Discovery data was successful. One of the things Network Discovery needs to communicate with you is your contact data. The Network Discovery Administrator sets up this information when creating your account. You may change any of these properties, to ensure that your contact information is up to date.

- E-mail address (optional, but required if the user is to receive any e-mail about the Peregrine appliance or the network)
- Pager e-mail address
- Pager number
- Pager service provider

To modify your contact data

- ▶ Click **Administration > My account administration > Account contact data.**

To enable e-mail notification

- ▶ Enter an e-mail address in the E-mail address field.

If the e-mail address is blank, the user will not receive any e-mail, even when the receive list box is set to “yes”.

To enable pager notification via an e-mail gateway

- ▶ Enter a pager address in the Pager e-mail address field.


To enable direct alphanumeric pager notification

- 1 Enter a pager number.
- 2 Select a pager service provider from the list box.

Note: The list of pager service providers must be created by the Network Discovery Administrator. See *Setting up Paging* on page 117.

3 Click **Modify Contact Data**.

Figure 4-2: Modify contact data



E-mail address:

Pager e-mail address:

Pager number:

Pager Service Provider:

Modifying your password

The Network Discovery Administrator may change the passwords occasionally, but this option gives you control over your own password. If you have trouble accessing your account, ask the Network Discovery Administrator to make sure you have the correct password.

Passwords can be up to 20 characters long. Acceptable characters are:

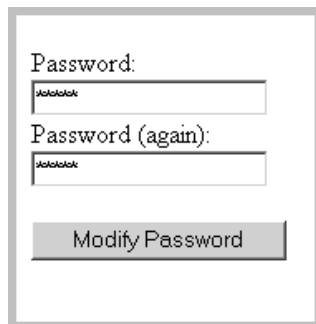
- A through Z
- a through z
- 0 through 9
- underscore (_)
- at (@)
- period (.)
- hyphen (-)

To change your account password

- 1 Click **Administration > My account administration > Account password**.
- 2 Enter the new password in the Password field.
- 3 Enter the new password in the Password (again) field.
- 4 Click **Modify Password**.

Note: When you change your password, you will be prompted to log in again using the new password.

Figure 4-3: Modify password



The screenshot shows a form with two text input fields. The first field is labeled "Password:" and contains a masked password "XXXXXXXX". The second field is labeled "Password (again):" and also contains a masked password "XXXXXXXX". Below the fields is a button labeled "Modify Password".

Testing your e-mail address

Testing your e-mail address will send an e-mail message to your account, so that you can:

- test that you have entered your e-mail address correctly
- test that the Peregrine appliance has been configured to send e-mail

To test your e-mail address

- 1 Click **Administration > My account administration > Test e-mail address**.
- 2 To send an E-mail message to your account, click **Confirm**.

Figure 4-4: Test e-mail address



The screenshot shows a confirmation dialog with the text "Send a test e-mail to admin@example.com?" and a button labeled "Confirm".

Testing your pager address

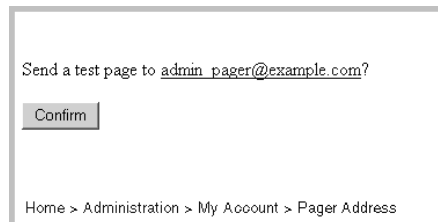
Testing your pager address will send an e-mail message to your pager, so that you can:

- test that you have entered your pager address correctly
- test that the Peregrine appliance has been configured to send e-mail

To test your pager address

- 1 Click **Administration > My account administration > Test pager address**.
- 2 To send an E-mail message to your pager, click **Confirm**.

Figure 4-5: Test pager address



Testing your pager number

Testing your pager number will send a test message to your alphanumeric pager through the dialup service provider.

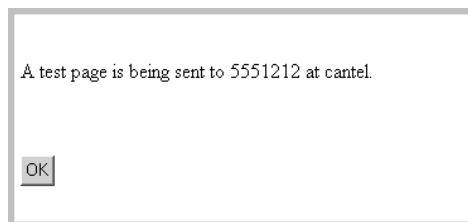
This will test that your pager is working and that the dialup service provider has been configured correctly.

To test your pager number

- 1 Click **Administration > My account administration > Test pager number**.

- 2 To send a message to your pager, click OK.

Figure 4-6: Test pager number



5 | A Tour: Toolbar, Health Panel, CHAPTER | Network Map

This chapter and the next provide a brief introduction to Network Discovery and how you can use it.

Topics in this chapter include:

- *The Toolbar is the starting point* on page 46
- *See an overview with the Health Panel* on page 48
- *The Network Map provides a graphical view* on page 51
- *What are the icons on the map?* on page 54

The Toolbar is the starting point

Once you have successfully logged into Network Discovery, you will see the Home page and Toolbar. The Toolbar is the center of navigation in Network Discovery; you can use the Toolbar to access all of the features of Network Discovery.













Figure 5-1: Toolbar



Navigating with buttons and links

Depending on your license, the Network Discovery 5.0 Toolbar has 12 or 16 buttons. If your license includes an Aggregator, your Aggregator Toolbar has one extra row of four buttons above the buttons included in the regular Toolbar. For more information on the Aggregator, see *Using an Aggregator* on page 189.

Table 5-1: Regular Toolbar buttons

	Health Panel		Status
	Network Map		Reports
	Service Analyzer		Administration
	Events Browser		Help
	Find		Close
	Home		Exit

These buttons are duplicated as a row of hyperlinks called the navigation bar at the bottom of the main browser windows. It is there for ease of navigation when you have several windows open.

Figure 5-2: Navigation Bar (Home page and an example)



Above the navigation bar is another row of links that shows you the path you have taken through the menus. On the Home page, this “pathway” row says “Home,”

On Administration, Reports, Status, and Help pages, the “pathway” links show the path you have taken to the HTML-based page you are on now.

See an overview with the Health Panel



The Health Panel enables you to set up, highlight, and examine conditions, faults, and statistics that Network Discovery has gathered about your network.

Note: The Health Panel is automatically updated with current device information.

Note: If you have an Aggregator, see *Using the Aggregate Health Panel* on page 199.

Opening the Health Panel

You can open the Network Map and Health Panel from four places:

- the Toolbar
- the Home page
- the navigation links
- the Tools menu on the Network Map (and vice versa—you can open the Network Map from the Tools menu of the health Panel)

You can minimize the Health Panel

When you first open the Health Panel, it appears in the detailed view. If you would like to shrink the Health Panel and view a summary of alarms and warnings, click the arrow button in the bottom right hand corner.

The brief view offers you a choice. You can see an overview of all the alarms and warnings on the network or you can select a fault category button to monitor a specific fault category.

If you would prefer to see one of the brief Views whenever you open a map session, you can change the preference in **Edit > User Preferences > Health Panel**.

Report buttons on the Health Panel show overall performance

To view a Health Panel report, click the report button next to the category of information you want, for example Line Breaks or Changes. All reports provide one row of data for each current alarm or warning in the network. Health Panel reports are automatically updated with the current event information.

The statistics near the bottom of the Health Panel provide you with critical information on the overall performance of the network.

Buttons for the performance of Network Discovery

The two buttons at the bottom of the Health Panel, **Exceptions** and **Appliance**, indicate whether Network Discovery is having problems mapping your network.

The Exceptions report

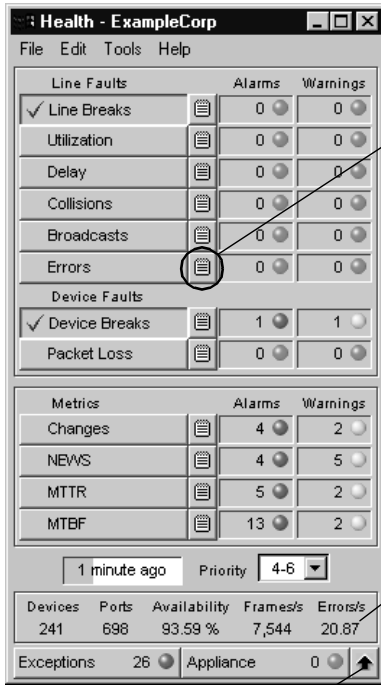
The Exceptions report indicates problems with your network that the network administrator can address—specifically, problems with misconfigured netmasks and with non-standard SNMP MIBs.

The Appliance report

The **Appliance** report indicates problems with your Peregrine appliance. These are problems that Peregrine Systems Customer Support will help you fix.

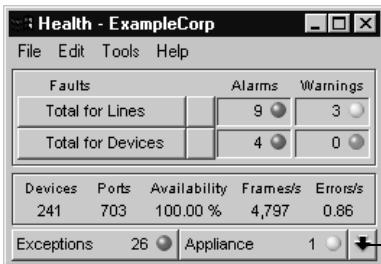
Figure 5-3: Health Panel

Detailed View of Health Panel



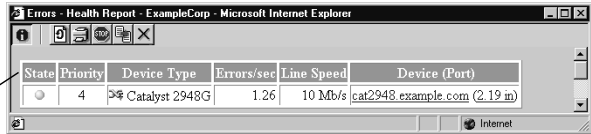
Click to shrink the Health Panel

Brief View of Health Panel



Click to enlarge the Health Panel

Health Panel report



Statistic	Explanation
Devices	The number of objects in the network.
Ports	The number of ports in your network
Availability	This number represents the number of devices with priority 3 (or higher) that are operational as a percentage of the total number of devices with priority 3 (or higher).
Frames	This number represents the instantaneous number of frames per second seen on the entire network.
Errors	This number represents the instantaneous number of errors per second seen on the entire network. This includes the number of errors on both the "in" and the "out" ports of the network devices.

The Network Map provides a graphical view



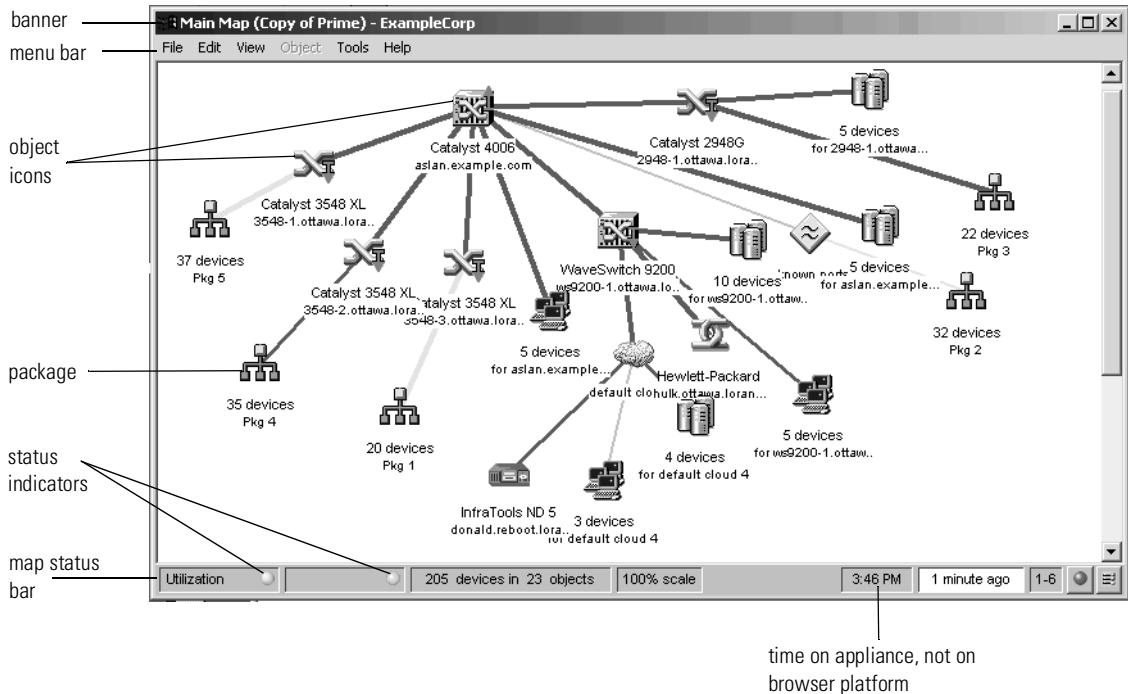
The Network Map provides a graphical view of the network, or a portion of it. The map shows icons that represent devices and lines that represent the connections between the devices.

Network Discovery collects data from the devices in your IP range, and uses this data to determine the type of each device, where it resides in your network, and to what other devices it is connected.

If you use Peregrine's Express Inventory, the WMI collector, to collect data on your network devices, you may have devices on your Network Map for which the only data collected is from the scan files. For more information on how to use Peregrine's Express Inventory, the WMI collector, see your ServiceCenter Essentials documentation.

If your license includes Map windows have several features that you can use, in conjunction with the Health Panel, to view the state of the network.

Figure 5-4: Network Map — Line Faults only



To determine what the Map will display, select a fault or metric by clicking a button on the Health Panel or by right-clicking the map status bar. Colored rings appear around the icons to indicate the objects' status for the category you selected.

The colored ring around an icon indicates the device's status for the category you select. For example, if you select MTBF from the Health Panel list or by right-clicking the map status bar, the devices that have alarms for their Mean Time between Failures will have red rings and the devices that have warnings will have yellow rings.

Note: To show rings the objects must meet the minimum priority as set on the Health Panel. (Information about setting priorities is in *Changing the priority of a device* on page 90.)

Note: Virtual devices do not show colored rings.

Note: “Scanned-only” devices from Peregrine’s Express discovery, the WMI collector, do not show colored rings.

There is more detail about faults in the *Reference Manual*.

Status Bar

The Status Bar appears at the bottom of every map window. It displays information about the window contents, and allows you to change the window display.

The following graphic shows the Status Bar. The table below the graphic explains the features available on the Status Bar.

Note: Some parts of the Status Bar duplicate information available on the Health Panel.

For more information on these components, see the *Network Discovery Reference Manual*

Figure 5-5: Status bar

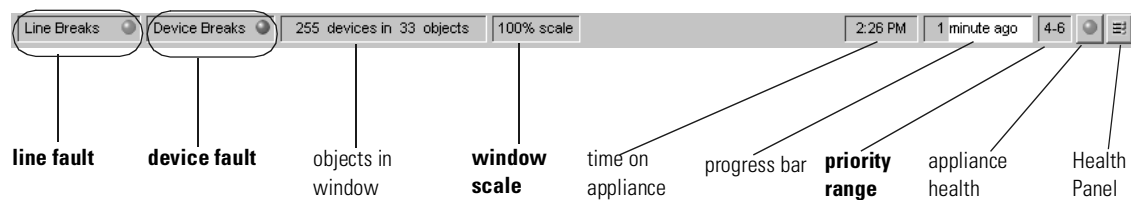
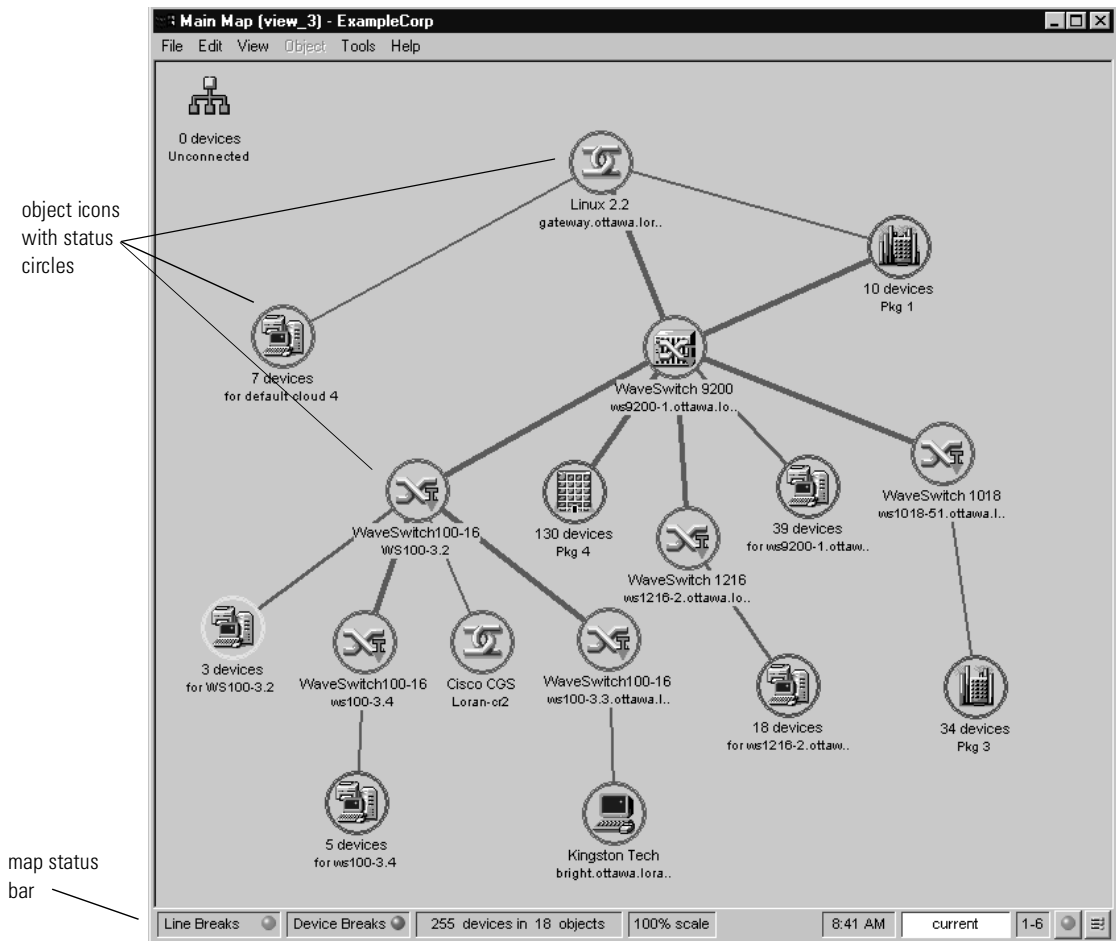


Figure 5-6: Network Map - Line Faults and Device Faults selected



What are the icons on the map?

The icons on the map fall into categories:

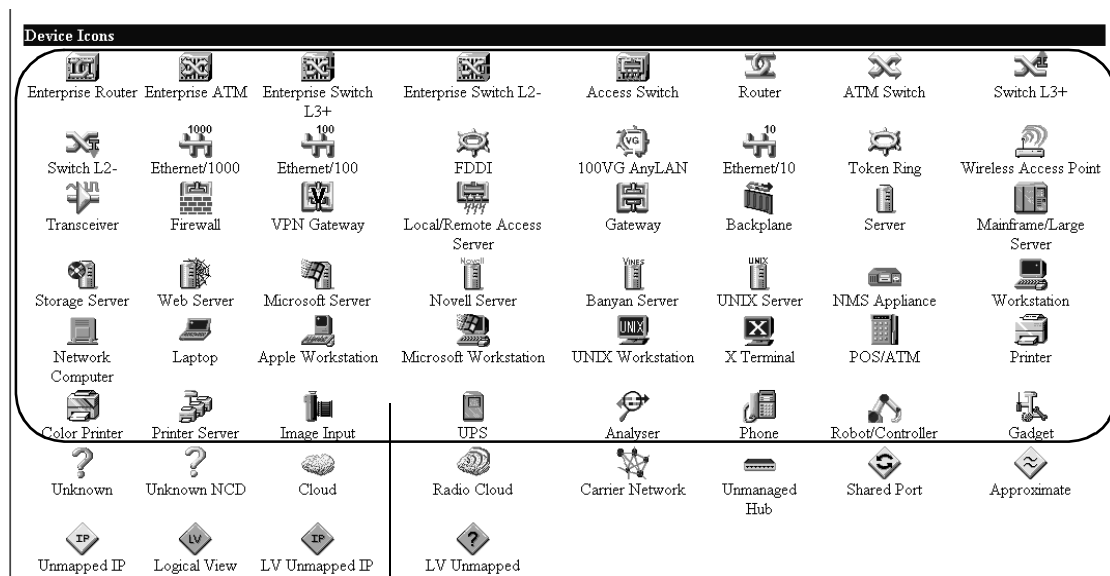
- device icons
- package icons
- cloud icons
- diamond icons

You can see a complete list of all the icons used in Network Discovery in **Help > Icons**.

Device icons

Device icons represent the physical equipment in your network.

Figure 5-7: Device icons as shown in Help > Icons



Device icons

Package icons group other icons together

Network Discovery helps you organize and simplify your Network Map with packages. A package is a collection of objects (objects means either devices or packages) that is represented by an icon. You can double-click a package icon to open the package in its own window. There are two types of packages:

- End node packages
- Multi-object packages

Any map window can contain packages. You can modify the contents of a package (selecting objects or groups of objects) exactly as you can in the Main Map.

For more information on packaging, see *Packaging Your Network* on page 101.

As with other icons, you will sometimes see package icons with colored rings around them (when you select fault category buttons). The color of the ring around the package depends on the color of rings around objects inside the package. The ring around the package icon will match the most severe instance of its contents.

For example, if there are Alarm (red), Warning (yellow) and OK (green) rings inside a package, the package will have an Alarm (red) ring.

Figure 5-8: Package icons as shown in Help > Icons



Virtual device icons show that connectivity is not clear

When Network Discovery is unable to determine the exact physical, port-level connectivity between devices, it displays the connection with a virtual device icon representing the logical subnet.

Network Discovery creates two types of virtual devices: clouds and diamonds.

Clouds represent one or more devices or MAC systems that provide connectivity in the network.

Diamonds do not represent actual network devices; they indicate connectivity. Sometimes, Network Discovery knows that there is connectivity without being able to specify the devices.

Clouds

There are 4 cloud icons.



- The “Cloud” icon represents one or more unmanaged devices that somehow connects two or more devices. Network Discovery has determined that two or more devices are indirectly connected to each other, but cannot get any information on the device or devices that implements the connection.



- The “Radio Cloud” icon represents a wireless network connection.



- The “Carrier Network” icon represents a carrier service provider, such as a third party network that is composed entirely of unmanaged devices.



- The “Unmanaged Hub” icon represents the single hub device that connects two or more devices, but Network Discovery cannot get any information from the MIB of that hub. The hub may not have SNMP management enabled, or perhaps Network Discovery has not been configured with its community string.

Diamonds

There are 6 diamond icons.



- The yellow “Unmapped IP” icon collects devices that belong on the same logical subnet, connected to a router, but for which Network Discovery has not yet determined the physical connection. The “Unmapped IP” icon has as its title the IP address of the subnet.



- The yellow “Approximate” icon is used to connect devices that Network Discovery believes to be connected to a switch or hub although Network Discovery does not know the ports to which the connections should be made. Network Discovery connects the hub or switch to an “Approximate” connection diamond and connects the diamond to the devices.



- The yellow “Shared Port” icon collects together the multiple devices that Network Discovery has seen attached to a single port. For example, you could see a yellow “Shared Port” icon when one port is used to test the operation of many different workstations, linked in sequence—perhaps in a test lab. Another example could be many people, each with a different laptop, sharing a common office.



- The orange “Logical View” icon collects all devices that are connected to other orange diamond-shaped icons, and connects them to the Peregrine appliance icon on your map. Device icons are not normally connected directly to the “Logical View” icon, rather they are connected to one of the two other orange icons described below.



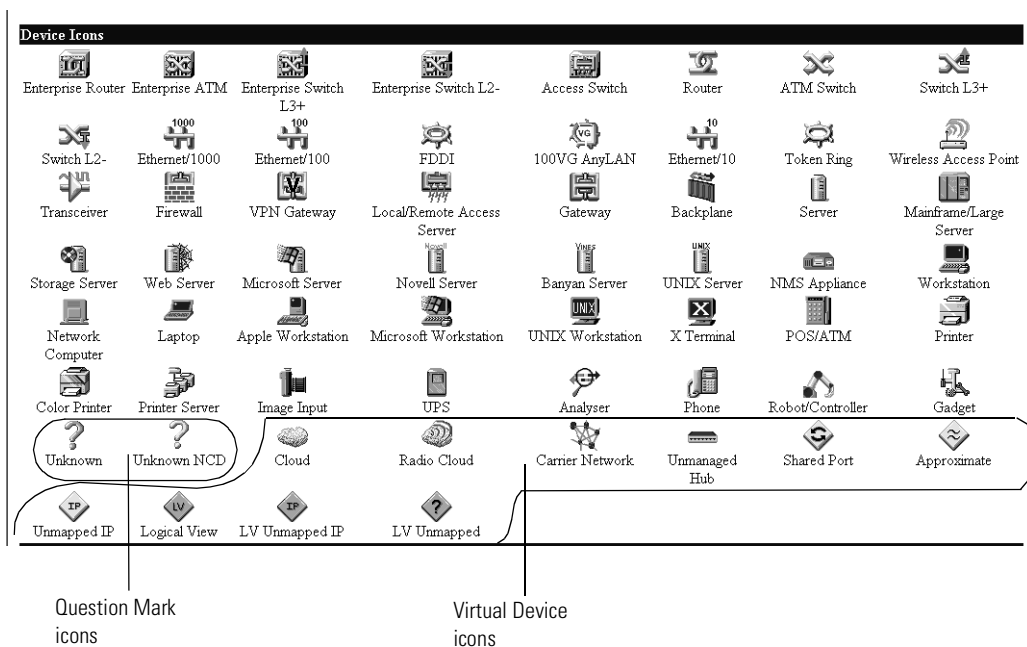
- The orange “LV Unmapped IP” icon collects devices that belong on the same logical subnet, but for which Network Discovery has not yet determined the physical connection, nor can it determine the appropriate router for that subnet. What is the difference between yellow and orange “Unmapped IP” icons? Yellow ones are attached to the appropriate router and orange ones are attached to the “Logical View” icon.



- The orange “LV Unmapped” icon collects together devices which Network Discovery has no idea how to connect; not even the subnet of the devices can be determined.

If you are using Peregrine's Express Discovery, the WMI collector, there will likely be scanned devices for which Network Discovery cannot monitor connectivity. The scanned devices may appear attached to the Logical View Unmapped icon. This is normal. If you wish, you can manually connect these devices to other devices on your Network Map. See *Forcing objects to be connected differently* on page 94.

Figure 5-9: Question Mark and Virtual Device icons as shown in Help > Icons



Other Icons

Question Mark Icons

There are two types of question mark icons. The yellow question mark icon represents a device Network Discovery can partially identify and believes to be a network connectivity device (such as a router or switch). A yellow question mark icon represents an Unknown Network Connection Device (Unknown NCD).

The gray question mark icon (Unknown) represents a device for which Network Discovery has only an IPv4 address.

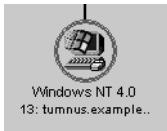
Question mark icons indicate a lack of information. If question mark icons remain for a few hours, a Network Discovery Administrator should check the Exceptions report to see what problems can be solved to make the network and Network Discovery work better.

The Network Discovery Administrator may decide to change the icons for Unknown devices or Unknown Network Connection Devices. If the Network Discovery Administrator changes the icon, all views of the map will be updated.

Figure 5-10: Question mark icons



Colored Ring



If an object has a colored ring drawn around it, it is because one of the Health Panel fault category buttons has been pressed, and the object meets the minimum priority as set on the Health Panel. By default, only devices with priorities 3 to 6 will have a colored ring drawn around them. If no icons have rings, it may be because you have not selected any fault category buttons on the Health Panel, or because none of the devices are above the minimum priority.

Note: If you are using Peregrine’s Express Inventory, the WMI collector, “scanned-only” devices appear without colored rings.

Gray Background



If an object appears with a gray background, or a gray icon, that means Network Discovery has not seen that device for more than 24 hours. Network Discovery will eventually trash such a device from the Network Map and, eventually, Network Discovery will purge the device and all its associated data.

Note: If you are using Peregrine’s Express Inventory, the WMI collector, “scanned-only” devices appear without grey backgrounds or gray icons.

Locked Icons



If you have manually packaged your map configuration, you will see many icons with a blue line beneath them, if you have selected the “Underline locked objects” option in **Edit > User Preferences**. The blue line indicates that the device has been manually packaged by a user, meaning it has been put inside a package (**Package** command), promoted from a package (**Up a Level, Promote**), or has had its package removed (**Unpackage**).

Network Discovery does create some automatic packages. They are created during discovery and whenever you use the **Pack** or the **Unpack All** commands.

For more information on packaging, see *Packaging Your Network* on page 101.

The behavior of “scanned-only” devices

A device can be:

- A network device that is discovered and monitored by Network Discovery only (by pinging, polling, and table reading).
- A network device that is automatically scanned by the WMI collector only
- A device that has been scanned by the WMI collector, is not on the network, and has had its scan file dropped into the shared folder in the Peregrine appliance.

“Scanned-only” devices appear on the Network Map integrated as well as possible with “discovered” devices. A scanned-only object usually has an IP address and if it does, it will appear on the map, connected to a Logical View diamond.

Scanned-only devices act the same way visually as discovered devices except that they do *not*:

- show rings, no matter what priority is selected
- appear in Health Panel reports
- turn gray when they have not been discovered for 24 hours

6 | A Tour: Managers, Events Browser, Service Analyzer, Reports

CHAPTER

This tour provides a brief introduction to Network Discovery's tools and how to use them to find and prevent problems.

Topics in this chapter include:

- *The Device Manager* on page 64
- *The Events Browser* on page 70
- *The Service Analyzer* on page 72
- *Find* on page 75
- *Administration* on page 78
- *Reports* on page 78
- *Status* on page 81

The Device Manager

The Device Manager offers details about the past and present state of a device. You can use the Device Manager to research the history of a device, or to interface with the device through its MIB.

You can access the Device Manager by double-clicking a device icon on the Network Map, or through hyperlinks available in other features.

Throughout the *Network Discovery User Guide*, we will explain how to use features of the Device Manager to achieve specific goals.

For details of all the buttons on the Device Manager, see the *Reference Manual*.

Figure 6-1: Sample Device Manager panel

Windows/2000 Workstation (Windows 2000) with 1 port with 1 connection
 loman.sales.example.com / 192.168.2.9
 priority 1

Exceptions:	● 1
Package:	Main Map > for ws1216-61.example.com
Operating system:	Windows 2000 (Type Unknown)
NetBIOS name:	WLOMAN
NetBIOS workgroup:	SALESGROUP
System OID:	.1.3.6.1.4.1.311.1.1.3.1.1
System OID manufacturer:	Microsoft
System description:	Hardware: x86 Family 5 Model 2 Stepping 12 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)
System contact:	Kim Lee [set]
System name:	LOMAN [set]
System location:	Sales area [set]
Read community string:	public
Write community string:	n/a

Attribute Name	Max Size	Thresholds	Unit
Breaks			
Downtime			time
Packet Loss	100.00		percent
Average Line In Utilization	100.00		percent
Total In Bytes			bytes/sec
Total In Frames			frames/sec
Total In Unicasts			frames/sec
Total Out Unicasts			frames/sec
Total In Broadcasts			frames/sec
Total Errors			frames/sec
Changes		6 alarm	hours
NEWS		180 alarm / 365 warning	days
MTTR			hours
MTBF			days

Port Index	MAC/IP	OUI/Netmask	Manufacturer/Domain Name
0 / Node	192.168.2.9	255.255.0.0	loman.sales.example.com
2 / Novell 2000 Adapter	00C0F0 3497F4	KINGST	Kingston Technology Corp
	192.168.2.9	255.255.0.0	loman.sales.example.com

Severity	Exception	Explanation
●	Device Has Lost SNMP Management	<p>Description: IND has detected that an SNMP agent in this device is no longer accessible. The SNMP agent may become inaccessible for one of the following reasons: Changes in the Community Strings or the Access List, A defect in the device that causes it to temporarily or permanently lose its SNMP agent (usually until the next reset or restart)</p> <p>Effect: No statistics can be collected from the device. Connection information cannot be verified, so over time connections to the device may be lost or become unstable.</p> <p>Action: If the community strings in the device have changed, add these to IND's community string list with an appropriate IP range. If the access list in the device has changed, ensure that IND's IP address is in the list. If the device configuration has not changed, then for a temporary solution, resetting or restarting the device will usually restore the operation of the SNMP agent. For a longer term solution, contact the device vendor for upgrade or replace with a device that does not exhibit this problem.</p>

Report as of Wednesday, May 23, 2001 11:13:53 EDT

The Port Manager



Like the Device Manager the Port Manager lets you drill down for detail about a problem. The Port Manager contains detailed information about a specific port.

To open the Port Manager click a hyperlinked port index number in the Device Manager.

The Attribute Manager

You can drill down still further with the Attribute Manager. You can find out the details about a specific characteristic or “attribute” of a device or port. Attributes include Breaks, Downtime, Packet Loss, Errors In, Errors Out, Data Delivery Ratio, for instance.

To see the complete list of Attributes

- ▶ Click **Help > Supported Attributes**.

To open the Attribute Manager for a device

- ▶ In the **Attribute Name List** of the Device Manager, Line Manager or Service Analyzer, click an Attribute name.

Figure 6-2: Attribute Manager for a Device

SNMP-managed device: Switch L2- (Catalyst 3548 XL) with 50 ports and 3 connections
3548-2.ottawa.loran.com / 172.22.1.251
priority 4

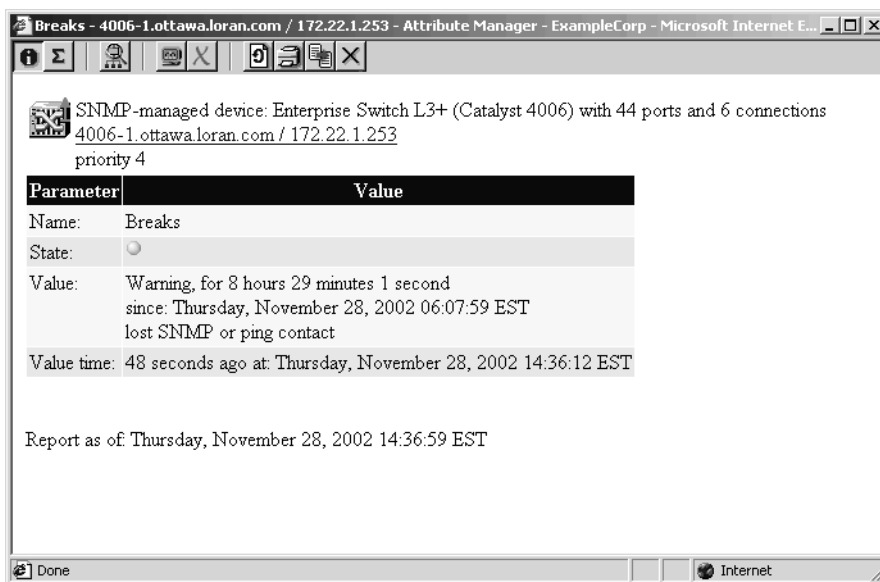
Parameter	Value
Name:	Breaks
State:	<input type="radio"/>
Value:	Warning, for 8 hours 23 minutes 28 seconds since: Thursday, November 28, 2002 06:07:56 EST lost SNMP or ping contact
Value time:	39 seconds ago at: Thursday, November 28, 2002 14:30:45 EST

Report as of Thursday, November 28, 2002 14:31:23 EST

To open the Attribute Manager for a port

- ▶ Click an Attribute Name from one of the following:
 - the Port Manager
 - the Line Manager
 - the Service Analyzer

Figure 6-3: Attribute Manager for a Port



The Line Manager

The Line Manager can appear in either of two modes:

- displaying multiple lines between
 - two devices
 - a device and a package
 - two packages
- displaying a single line between two devices

If you open a Line Manager with multiple lines, it appears as shown in Figure 6-4.

To open a single Line Manager, click on one of the arrows in the middle of the screen. You can also open Port Manager or Device Manager windows.

Note: You may notice that the statistics for these ports do not always match. This is because the statistics were collected at slightly different times.

Figure 6-4: Click an arrow on the Multiple Line Manager to open a single Line Manager for that line

Multiple line between device [aslan.example.com](#) and package [Building 2 switches](#)

Device Type	Device (Port)	Delay	Device Type	Device (Port)
Catalyst 4006	aslan.example.com (2.1)	↔	Catalyst 3548 XL	3548-1.ottawa.loran.com (117:1.2)
Catalyst 4006	aslan.example.com (2.2)	↔	Catalyst 3548 XL	3548-2.ottawa.loran.com (117:1.2)
Catalyst 4006	aslan.example.com (2.3)	↔	Catalyst 2948G	2948-1.ottawa.loran.com (2.49)

SNMP-managed device: Enterprise Switch L3+ (Catalyst 4006) with 44 ports and 6 connections
[aslan.example.com / 172.22.1.253 \(2.2 / short wave fiber gigabit ethernet\)](#) (user-assigned title)
 priority 4 [locate]
 Ethernet CSMA/CD at 1 Gbit/sec, Full duplex, Alarm type: Ethernet 1000 FD

SNMP-managed device: Switch L2- (Catalyst 3548 XL) with 50 ports and 3 connections
[3548-2.ottawa.loran.com / 172.22.1.251 \(117.1.2 / GigabitEthernet0/1\)](#)
 priority 4 [locate]
 Ethernet CSMA/CD at 1 Gbit/sec, Full duplex, Alarm type: Ethernet 1000 FD

Connection made via link training

State	Attribute Name	Unit	Value	State	Attribute Name	Unit	Value
Device:				Device:			
<input type="radio"/>	Breaks		Warning, for 9 hours 26 minutes 28 seconds since: Thursday, November 28, 2002 06:07:59 EST lost SNMP or ping contact	<input type="radio"/>	Breaks		Warning, for 9 hours 26 minutes 31 seconds since: Thursday, November 28, 2002 06:07:56 EST lost SNMP or ping contact
	Downtime	time	0 seconds		Downtime	time	0 seconds
<input type="radio"/>	Packet Loss	percent	n/a	<input type="radio"/>	Packet Loss	percent	0
	Average Line In Utilization	percent	0.05833		Average Line In Utilization	percent	0.03833
	Average Line Out Utilization	percent	0.1253		Average Line Out Utilization	percent	0.05333

The Events Browser



Network Discovery logs events in your network. An event is a change from one state to another: OK to alarm, OK to warning, warning to alarm, and so on. The categories of events correspond to the line and device fault categories on the Health Panel (Line Breaks, Utilization, Delay, Collisions, Broadcasts, Errors, Device Breaks, Packet Loss) plus two extra ones. The extra ones are “add” and “delete” for the events that occur when you (or Network Discovery) add or delete a device.

For example, Network Discovery can log an event if someone adds a device to the network. It may also log an event when a line breaks or if there are too many delays on a line. The Events Browser shows you a list of events that occurred on lines and devices in your network during a specified period.

The Health Panel and Network Map give you information about the current state of your network. The Events Browser gives you historical information. The Health Panel and Network Map can tell you what’s wrong now. The Events Browser shows you problems that only patterns over time can reveal.

The following affect what the Events Browser shows.

- Events filters. Event filters control what events are logged in the first place for you to view with the Events Browser. There is more information in *Setting up Event Filters* on page 129.
- Time. What period of time in the future or past do you want the Events Browser to show you?
- Settings in your Prime map configuration. The Events Browser is based on the Prime configuration and its device priorities. For more information on the Prime map configuration, see *Organizing Map Configuration Files* on page 109.
 - Alarm Thresholds. What does Network Discovery accept as a change of state? For example what threshold separates a warning from an alarm in a specific category like Utilization and, consequently, what qualifies as an event for the Events Browser?
 - Priorities. What priority of device should the Events Browser include?

To access the Events Browser:

- ▶ On the main Toolbar click the **Events Browser** button.
- OR

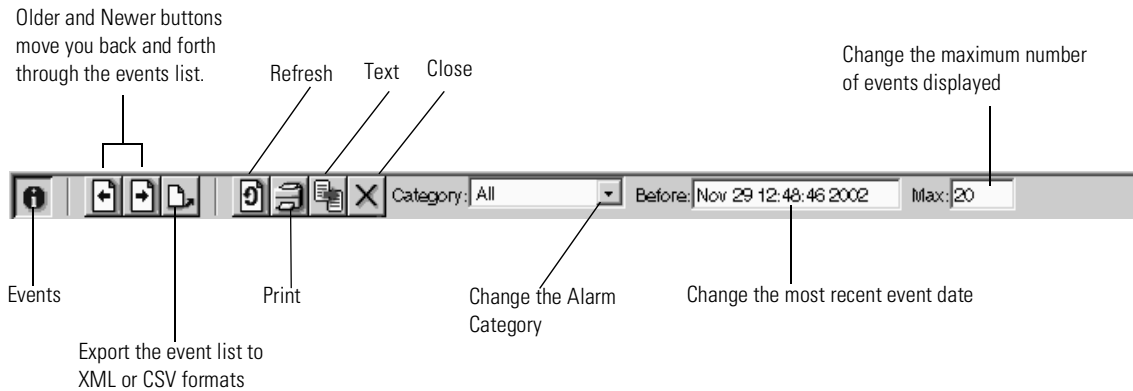
- ▶ On the Home page click the Events Browser
- OR
- ▶ From a map window or the Health Panel, click Tools > Events Browser.

Figure 6-5: Events Browser

Date/Time	State	Category	Priority	Device Type	Device (Port)	Value
2002-11-29 01:16	<input checked="" type="radio"/>	Collisions	4	Catalyst 2948G	2948-1 ottawa.loran.com (2.8)	0.06
2002-11-29 01:15	<input checked="" type="radio"/>	Collisions	4	Catalyst 2948G	2948-1 ottawa.loran.com (2.8)	208.81
2002-11-29 00:45	<input checked="" type="radio"/>	Collisions	4	WaveSwitch 9200	ws9200-1 ottawa.loran.com (113)	17.09
2002-11-29 00:44	<input checked="" type="radio"/>	Collisions	4	WaveSwitch 9200	ws9200-1 ottawa.loran.com (113)	510.31
2002-11-29 00:44	<input checked="" type="radio"/>	Collisions	4	Catalyst 3548 XL	3548-3 ottawa.loran.com (62.148)	23.86
2002-11-29 00:44	<input checked="" type="radio"/>	Collisions	4	Catalyst 3548 XL	3548-3 ottawa.loran.com (62.118)	28.42
2002-11-29 00:43	<input type="radio"/>	Collisions	4	Catalyst 3548 XL	3548-3 ottawa.loran.com (62.148)	75.78
2002-11-29 00:43	<input checked="" type="radio"/>	Collisions	4	Catalyst 3548 XL	3548-3 ottawa.loran.com (62.118)	125.73
2002-11-29 00:24	<input checked="" type="radio"/>	Collisions	4	Catalyst 3548 XL	3548-3 ottawa.loran.com (62.148)	31.17
2002-11-29 00:24	<input checked="" type="radio"/>	Collisions	4	Catalyst 3548 XL	3548-3 ottawa.loran.com (62.118)	36.70
2002-11-29 00:21	<input type="radio"/>	Collisions	4	Catalyst 3548 XL	3548-3 ottawa.loran.com (62.148)	61.42
2002-11-29 00:21	<input checked="" type="radio"/>	Collisions	4	Catalyst 3548 XL	3548-3 ottawa.loran.com (62.118)	132.05
2002-11-29 00:20	<input checked="" type="radio"/>	Collisions	4	Catalyst 3548 XL	3548-3 ottawa.loran.com (62.148)	16.23
2002-11-29 00:20	<input checked="" type="radio"/>	Collisions	4	Catalyst 3548 XL	3548-3 ottawa.loran.com (62.118)	12.39
2002-11-29 00:19	<input checked="" type="radio"/>	Collisions	4	Catalyst 2948G	2948-1 ottawa.loran.com (2.8)	0.18
2002-11-29 00:18	<input type="radio"/>	Collisions	4	Catalyst 2948G	2948-1 ottawa.loran.com (2.8)	58.56
2002-11-29 00:18	<input type="radio"/>	Collisions	4	Catalyst 3548 XL	3548-3 ottawa.loran.com (62.148)	51.91
2002-11-29 00:17	<input checked="" type="radio"/>	Collisions	4	Catalyst 2948G	2948-1 ottawa.loran.com (2.8)	157.41
2002-11-29 00:15	<input type="radio"/>	Collisions	4	Catalyst 2948G	2948-1 ottawa.loran.com (2.8)	69.28
2002-11-29 00:13	<input checked="" type="radio"/>	Collisions	4	Catalyst 3548 XL	3548-3 ottawa.loran.com (62.148)	49.22

The following diagram of the Events Browser toolbar shows all the methods of changing the event list. You can use the different buttons and text boxes to view the events in which you are most interested.

Figure 6-6: Events Browser toolbar



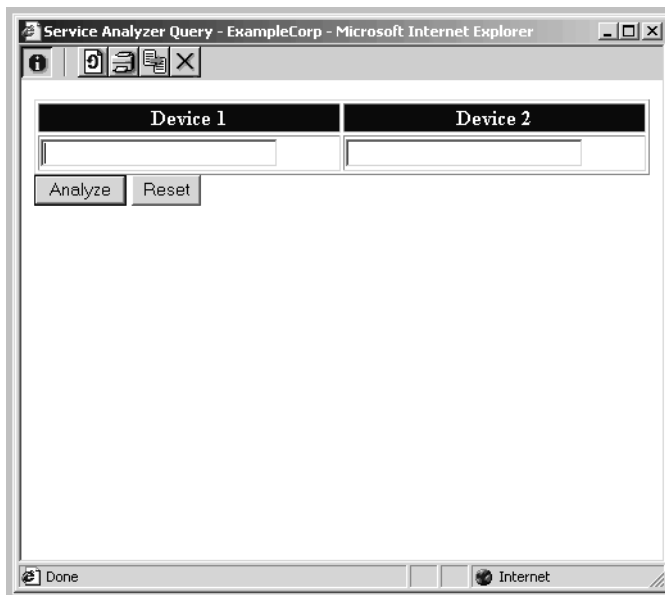
The Service Analyzer



The Network Discovery Service Analyzer allows you to analyze the network path between two devices. You enter the device names or IP or MAC addresses and Network Discovery displays a map of the network path between the two devices. By checking the status colors of the lines and devices in the object path, you can quickly determine where communication problems are occurring. Network Discovery also lists the service problems detected on the path.

To get started with the Service Analyzer, you must identify the devices at the ends of the path you want to analyze.

Figure 6-7: Service Analyzer Query window



To open the Service Analyzer

- ▶ On the main Toolbar click the **Service Analyzer** button.
 - OR
 - ▶ On the Home page click **Service Analyzer**.
 - OR
 - ▶ From a map window or the Health Panel, click **Tools > Service Analyzer**.
- 1 Enter identifiers for the objects. You can enter the IP address, MAC address, domain name, Net BIOS name, or device title.

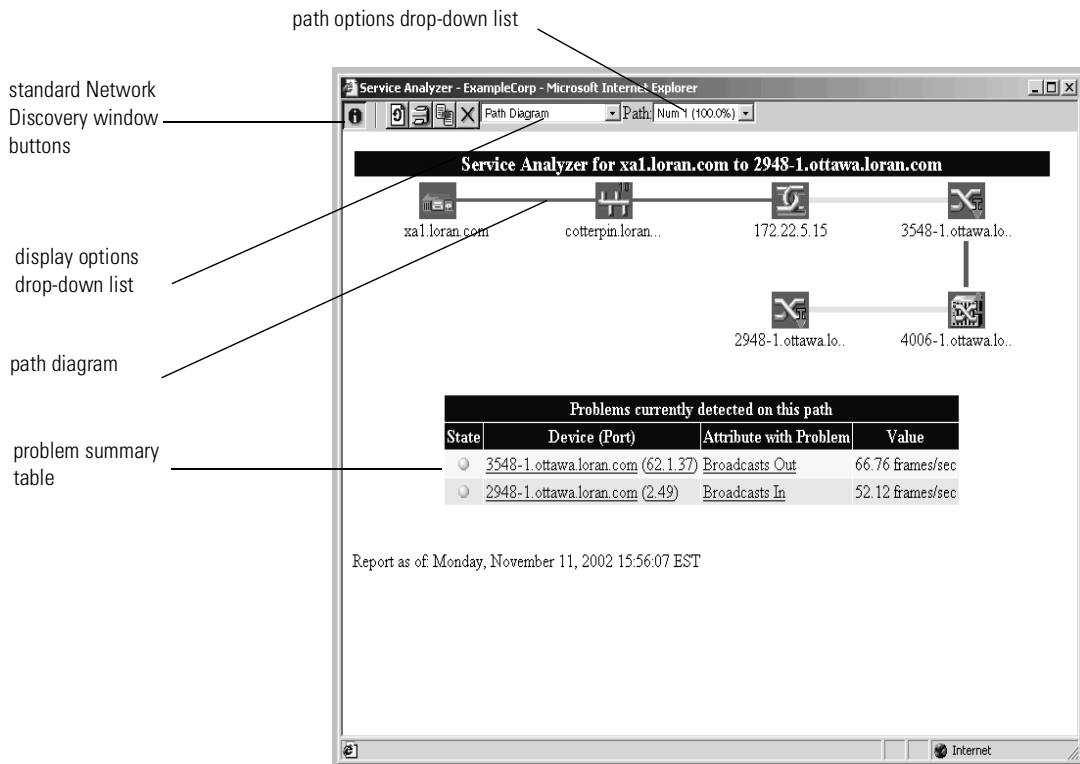
Note: The Service Analyzer cannot be used with packages, only with icons that represent a single device.
 - 2 Click the **Analyze** button.

Note: The Reset button clears the fields so that you can enter new identifiers.

The Service Analyzer window shows the path and a table listing currently detected problems. The remainder of this section discusses the functions available from the Service Analyzer window.

When it is first accessed, the Service Analyzer window displays the path between the two devices entered in the query window. Multiple views are available to display the data for different paths between the two devices. The Path Diagram is displayed first by default.

Figure 6-8: Service Analyzer Window



The window has the following options:

- Standard Network Discovery window buttons: including About, Refresh, Print, Stop, Text and Close.
- Display options drop down list: allows you to select the type of data displayed in the Service Analyzer window. The data is displayed in graphs.
- Path drop-down list: if Network Discovery detected multiple paths between the devices, you can select the path for which you want to display data.




- Path diagram: displays a map of how packets travel between the selected devices. The same status colors are applied to the icons and lines as applied in the Network Map. This path diagram allows you to quickly determine problem devices. By viewing the graphs under the other display options, you can determine the extent and impact of a problem on the communication between the selected devices.
- By clicking on a device icon or a line, you can access the Network Discovery Device Manager or Line Manager.
- Problem summary table: lists the problems that Network Discovery has detected on the network path.

Find



The Find command lets you locate and examine any device or port on the network. Find has three panels for searching your network:

- Device
- Port
- Advanced:

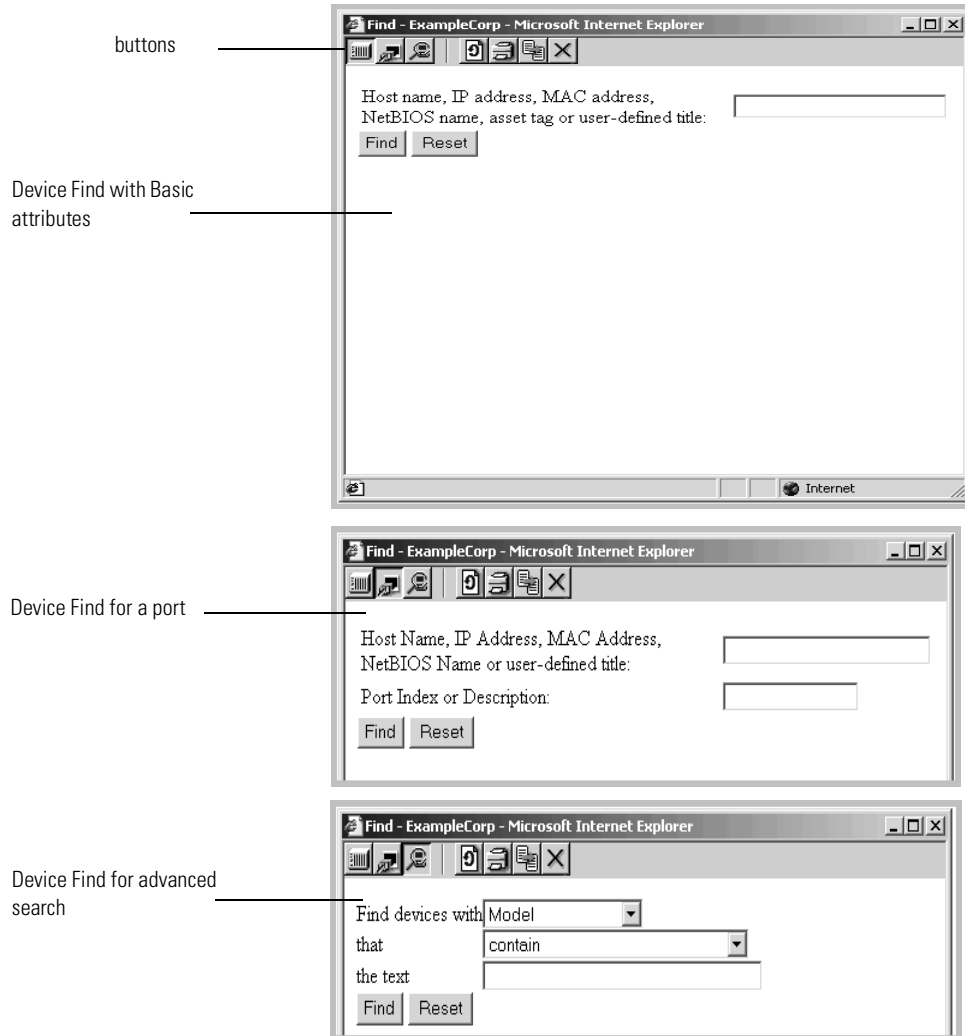
Button	Function
 Device	Allows you to search for a device by a basic attribute, such as Host Name, IP or MAC address, Net BIOS name, asset tag, or title.
 Port	Allows you to search for a port by basic device attribute and port attribute (port index or description)
 Advanced	<p>Allows you to use a wildcard to search on other attributes of a device. A description, contact, location, name (from SNMP), family, model, OS, application (from rule base) can all be used.</p> <p>Find devices with: allows you to identify the type of information on which you want to search. From the drop down list, you have the choice to search by model, operating system, application, and SNMP information.</p> <p>that: allows you to specify the type of query. The drop down list allows you to select: contain, begin with, end with, match exactly, match with wildcard, match using a regular expression.</p> <p>the text: allows you to enter a description of the device or devices you are trying to find.</p>

To use the Find tool

- ▶ On the main Toolbar click the **Find** button.
OR
- ▶ On the Home page click **Find**.
OR
- ▶ From a map window or the Health Panel, click **Tools > Find**.
 - 1 Click the button for the Find panel you want to open **Device, Port** or **Advanced**.
 - 2 Enter the search criteria.

Network Discovery searches for the device (or port). If Network Discovery finds one match, a hyperlink for the match is listed in the Find window and a Device Manager or Port Manager session opens. If more than one match is found, the Find window displays a list of hyperlinked device or port titles. Each link opens a Device Manager or Port Manager session.

Figure 6-9: The Find Window



Administration



You can reach the Administration page from the Home page, from the Navigation Bar, or from the Administration button on the Toolbar. IT Employee accounts can start from the Administration page to make changes to their own accounts and manage their map configuration files. The Administration page is also the starting point for many administrative tasks such as entering the network ranges to be covered by Network Discovery, setting up and modifying accounts, setting up paging, backing up Network Discovery data and so on.

Most of the tasks on the Administration page should have been done (by the Network Discovery Administrator) during the initial installation process but if you need to make changes, see the *Network Discovery Setup Guide*.

To learn about the options available in the administration pages, read the help associated with each page. For more technical information, refer to the *Network Discovery Reference Manual*.

Reports



Reports provide:

- historical data (about a problem that has occurred in the past or over time)
- graphical images that may be easier for you to understand
- presentation material that can be displayed to your manager or to people in other departments

The reports are divided into groups. In most of the groups, reports are available in two formats, summary and detailed. You also have a choice of reporting periods, such as yesterday, last week or last month.

All reports reflect the prime map configuration and its packaging (except, of course, Automated Inventory reports).

Executive Summary/Network Reports

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

To view the Executive Summary Network Inventory Reports

- ▶ **Reports > Network Documentation > Device Inventory Summary**
- ▶ **Or Reports > Network Documentation > Device Inventory**

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

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

You may not even know what you don't know! The Device Inventory Summary report tells you and the Device Inventory report tells you in more detail.

WAN Reports

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

To view a Data Delivery Ratio Report

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

LAN Reports

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

Device Reports

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

Support Reports

The Support Reports have to do with Network Discovery performance, especially exceptions. Exceptions are problems with your network that the network administrator can address—specifically, problems with misconfigured netmasks and with non-standard SNMP MIBs— problems that keep Network Discovery from working its best.

The Health Panel exceptions report gives you a summary of current exceptions in your network, really just telling you how many things are wrong and what kinds of problems there are. The Support Reports on the Reports page give you more detail, telling you exactly where the problems are.

You can use Network Discovery data with other applications

You may wish to customize reports to show to your management team. You can download graphs and pie charts of Network Discovery data into Microsoft Word documents.

You can also use your own data access application to customize the presentation of Network Discovery data, if your data access application operates on the Open Database Connectivity (ODBC) standard. ODBC applications into which you can export Network Discovery data comprise (but are not limited to):

- Crystal
- Cognos Impromptu
- PowerPlay OLAP tool

For more information on how to use Network Discovery data with Microsoft Word or with data access applications, see the *Data Export Guide*.

Status



Status shows you what the Network Discovery Administrator has done in the Administration part of Network Discovery. It tells you what Network Discovery is set up to do and how well it is doing it. It tells you things like:

- How the Peregrine appliance is doing
- How the network is doing
- What license(s) you have and how many map sessions are available
- How the Aggregator is doing
- What devices have been filtered out

7 Customizing Your View of the Network Map

CHAPTER

You can change the look of the Network Map at any time. Depending on what you need to accomplish with Network Discovery, you can change object icons, or change the appearance of lines.

Different account levels have different privileges and different levels of responsibility.

Topics in this chapter include:

- *Customizing for any accounts* on page 84
- *Customizing for IT Manager and Administrator accounts* on page 91

Customizing for any accounts

The following customization changes only affect map configurations of the person who makes them, unless the user has an IT Manager or Administrator account and saves the configuration as the Prime configuration. For more information, see *Organizing Map Configuration Files* on page 109.

Some of the changes affect only the map configuration you are looking at now; some affect how you view any map configurations.

Renaming an object

You can give an object a descriptive title instead of the IP address, MAC address, or domain name. The new name will only be in your current map configuration.

To rename an object

- 1 With a device selected, **Object > Properties**.
- 2 In the Properties dialog, enter a title in the “Enter new title” field.
- 3 Click OK.

To reset to the default title

- 1 Click the “Use default title” check box.
- 2 Click OK.

Customizing how you see the map

You can change the look of your Network Map in several ways. These preferences will affect how you see all of your map configuration files.

Changing the line style

Line style enables you to select which style of line to draw to connect objects in a Network Map window. You can change this setting from the default (straight) whenever you wish.

To change the map line style

- 1 From the **Edit** menu, choose **User Preferences**.
A dialog appears, from which you can change the line style.
- 2 Click one of the following:

- Step
 - Straight
 - Zigzag
- 3 Click OK.

Changing the color of the map background

To change the map background color preference

- 1 From the **Edit** menu, choose **User Preferences**.
A dialog appears, from which you can change the map color.
- 2 Click one of the following:
 - Olive
 - Black
 - White
 - Gray
- 3 Click OK.

Changing the map scale

You can change the scale for all map windows by changing the scale preference, or you can change each window individually. Select one of the following procedures.

Change scale for all windows

You can set a preference for all your Network Map windows, so they will all appear at a specific scale.

To change the map scale preference (for all windows)

- 1 **Edit > User Preferences**.
A dialog appears, from which you can change the map scale.
- 2 Click one of the following:
 - 300%
 - 200%
 - 150%
 - 100%
 - 75%

- 50%
 - 25%
- 3 Click OK.

Change scale for one window

You might want to see the entire network on one screen, or you might want to zoom in on a specific part of the network. The following quick procedures will show you how to view the Network Map from different perspectives.

This change to the scale for one window is temporary. The next time you open a map window, it will open at the size you set when you “changed the scale for all map windows,” (or, if you have not changed the setting, it will open at the default of 100%.)

To view all the objects at once

- ▶ View > Fit Map to Window.

To eliminate unwanted blank space

- ▶ View > Fit Window to Map.

To zoom in or out of the map

- 1 View > Scale.
- 2 Click one of the following:
 - 300%
 - 200%
 - 150%
 - 100%
 - 75%
 - 50%
 - 25%

Changing other viewing preferences

Show pop-up info

- 1 Edit > User Preferences >Map.
- 2 Click the box beside Show pop-up info.

Underline locked objects

- 1 **Edit > User Preferences >Map.**
- 2 Click the box beside **Underline locked objects**.

Confirm packaging commands

When you perform packaging commands such as:

- Layout
- Make Top of the Network
- Pack
- Unpack

you receive a confirmation question that gives you time to reconsider what you are doing. You can turn confirmation messages off, if you wish.

To set Network Discovery to ask (or not ask) for confirmation before completing packaging commands.

- 1 **Edit > User Preferences >Map.**
- 2 Click the box beside **Confirm packaging commands**.

Shade icons when selected

You can set Network Discovery to shade icons when they are selected. Otherwise, the icons will have the outline of a box around them. (There is still visual indication that the icon is selected.) By default, “shade icons when selected” is turned off because shading takes more memory and doesn’t work well with Microsoft Windows 95.

- 1 **Edit > User Preferences >Map.**
- 2 Click the box beside **Show icons when dragging**

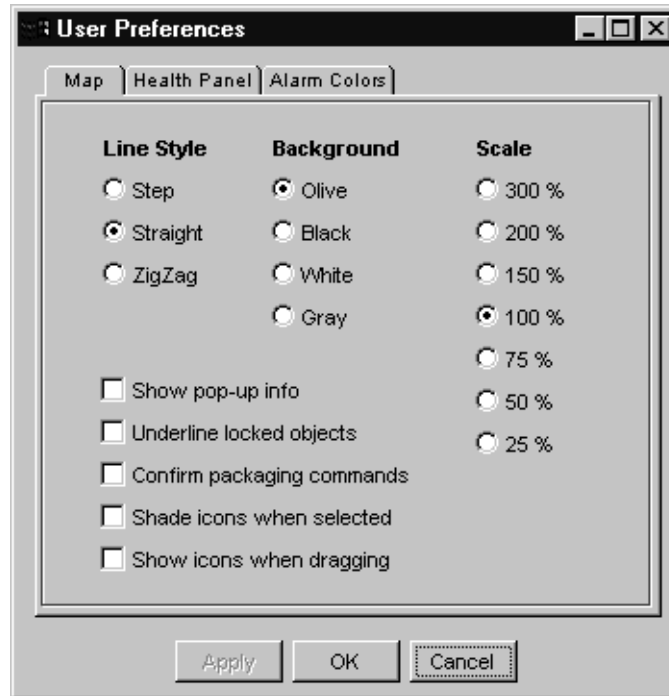
Show icons when dragging

When you are customizing your Network Map, you will likely be moving icons, and groups of icons around the screen. You can choose how the groups of objects will appear as you drag them around the map window.

To have icons show when they are being dragged in the Main Map

- 1 **Edit > User Preferences >Map.**
- 2 Click the box beside **Show icons when dragging**.

Figure 7-1: User Preferences dialog



Customizing alarm and warning colors

The colors selected for alarms and warnings are used in many areas of Network Discovery:

- rings around device icons on the Network Map
- LEDs in the Health Panel
- LEDs in the Reports and Status menus
- panels in the Device Manager, Line Manager, Port Manager, and Attribute Manager
- lines and background in the Service Analyzer

You can change the default colors if you wish.

To change the colors

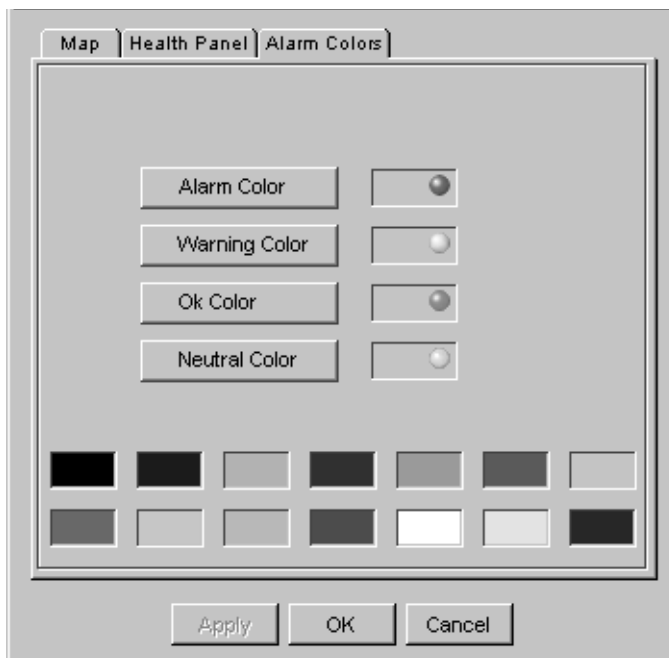
With either the Network Map or Health Panel open,

- 1 From the **Edit** menu, choose **User Preferences**.

The User Preferences dialog appears.

- 2 Click the **Alarm Colors** tab.
- 3 The Alarm Colors dialog opens

Figure 7-2: The Alarm Colors dialog



- 4 Select one of the buttons (for example, Alarm color).
- 5 Select one of the colors from the palette.
- 6 Click **Apply** or **OK**.

Placing an object at the top of the map window

When you are organizing a map window, you can assign one object to appear at the top of the window. This object should be of special significance in relation to the other objects in the window.

Network Discovery may not have been running long enough to show the right device at the top of the map or you may know a top-of-network router or a core device would make more sense, you can assign it to appear at the top of the map.

This preference will affect the current map configuration file.

To place an object at the top of the map window

- 1 Click an icon.
- 2 From the **Object** menu, click **Properties**.
- 3 Click the “Make this the top object in the current network package” check box.
- 4 Click **OK**.

The window is redrawn with the selected icon at the top.

To reset the top object for the window to the default chosen by Network Discovery

- 1 Click the icon at the top of the map window.
- 2 From the **Object** menu, click **Properties**.
- 3 Click to clear the “Make this the top object in the current network package” check box.
- 4 Click **OK**.

If the check box is already clear, then the top object is already the default.

Changing the priority of a device

You might increase the priority of a device that is important to you or a device that you will want to monitor more closely. This preference will affect the current map configuration file.

Devices with priority 6 are the most important. The higher the number, the higher the priority and the greater the importance.

Warning: Warning for Administrator accounts. If you are changing the priority of a device in the Prime map configuration, you may affect your event filters. (For more information on event filters, see *Setting up Event Filters* on page 129.)

To change the priority of a device

- 1 Click an icon.
- 2 From the **Object** menu, click **Properties**.

The Device Properties window appears.

- 3 Select a priority level in the Device Priority field.
- 4 Click OK.

Customizing for IT Manager and Administrator accounts

This section is for IT Manager and Administrator accounts only. IT Manager and Administrator accounts can also perform all of the procedures described in the section, *Customizing for any accounts* on page 84.

IT Manager and Administrator accounts can make changes to the Network Map that affect what all accounts see.

Changing a device icon

This procedure allows the user to replace the icon of the selected device.

Warning: Only IT Manager and Administrator accounts can change a device icon. The changed device icon is seen by all users in all map configurations.

Warning: Changing a device icon changes its device type, which can change its priority. A device's default priority is determined by its icon. Unless the device priority is explicitly set in a configuration, the device priority changes when the icon changes. See *Changing the priority of a device* on page 90.

If you are working in the Prime map configuration, changing a device icon and priority affects your event filters. See *Setting up Event Filters* on page 129.

Changing a device icon affects what reports the device appears in.

Note: Changing a device icon can change how it is packaged. Certain icons are classified as end nodes, which are packaged automatically. When you change an end node icon to an icon that is not an end node, the device can be automatically unpacked. If you change a device icon to an end node icon, that device can be automatically packaged with the end nodes.

To open the Properties dialog if a map session is in progress

- 1 With a device icon selected, click **Object > Properties**.

The Properties dialog appears.

- 2 Select a new icon for the device.
- 3 Click **Apply**.
- 4 Click **OK**.

Note: It can take a few minutes (depending on the size of your network) for a new icon to have full effect.

To open the Properties dialog if no map session is in progress

- 1 Click **Find** on the Toolbar.
- 2 Enter a device name, and click **Find**.

A Device Manager session opens for that device

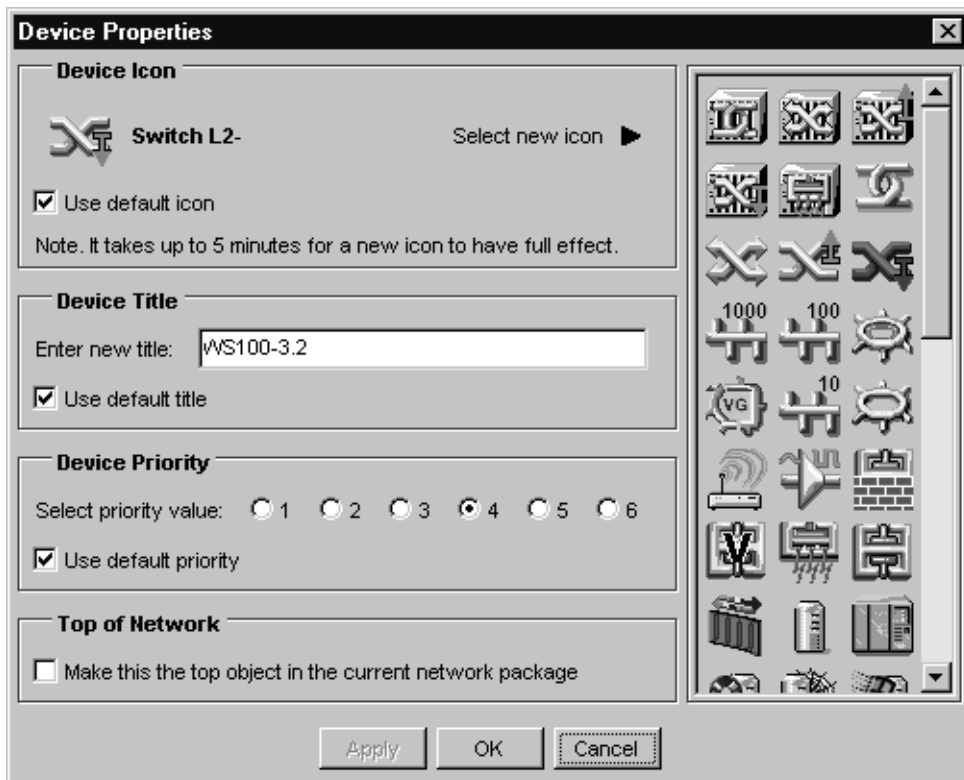
- 3 Click the **Properties** button on the Device Manager.
- 4 Click **OK**.

The Main Map window opens and the Device Properties dialog appears.

- 5 Select a new icon for the device.
- 6 Click **OK**.

Note: It can take a few minutes (depending on the size of your network) for a new icon to have full effect.

Figure 7-3: Device Properties window



To reset the device icon to the default chosen by Network Discovery

- 1 In the Device Properties dialog, click the “Use default icon” check box.
- 2 Click OK.

The icon changes within the map window.

A dialog box appears, informing you how long the change will take to complete.

- 3 Click OK.

Note: Changes to device icons do not appear on the map for a few minutes.

Customizing map contents

As you learn more about your network, and as the network expands, you may need to purge some devices or add some new devices. If Network Discovery has not created its network connections properly, you may want to force new connections on the Network Map.

Purging objects

The Purge command adds a device to the list of devices to be purged.

To purge a device—from the Network Map

- 1 Select a device on the Network Map
Object > Purge.

A confirmation dialog appears.

- 2 If you are sure you want to purge the device, click **Purge**

To purge a device—from the Device Manager

- 1 From the: Device Manager, click the Purge button.

A confirmation dialog appears.

- 2 If you are sure you want to purge the device, click **Purge**

Note: If you click the Purge button in the Port Manager you delete a port. If you click the Purge button in the Attribute Manager, you delete an attribute.

Forcing objects to be updated

This button is available in the Device Manager. For more information on the Device Manager, see the *Reference Manual*.

Clicking the **Update Model** button allows an Administrator account user to put this device at the top of the device modeler's queue.

You would use this command when you have made changes to a device that affect connectivity—for example, when you have changed cards in a router, and do not want to wait for an automatic update.

To force an object to be updated

- 1 Open the Device Manager by double-clicking on a device in the Network Map.
- 2 Click **Update Model**.

Forcing objects to be connected differently

Create connection and **Break connection** buttons are available in the Port Manager. For more information on the Port Manager, see the *Reference Manual*. A **Break connection** button is also available in the Line Manager.

Create connection and **Break connection** do not change the physical connection on the device; they change only how Network Discovery represents the connection on the Network Map.

Warning: Do not create a connection without consulting your Network Discovery Customer Support representative. If you force a connection, Network Discovery may not be able to correctly connect your network devices.

To break an existing connection, from the Line Manager

- 1 Open the Line Manager by double-clicking on a line in the Network Map.
- 2 Click the **Break Connection** button. (The line must be active or the **Break Connection** button does not appear.)

The existing connection is displayed, with a confirmation question.

- 3 Click **Break**.
- 4 Click **Yes**.

To break an existing connection, from the Device Manager

- 1 Open the Device Manager by double-clicking on a device in the Network Map.
- 2 Click the **Ports** button to open the Ports panel.
- 3 From the Ports panel, click the port index you want to change.

A Port Manager window opens.

- 4 Click the **Break Connection** button.

The existing connection is displayed, with a confirmation question.

- 5 Click **Break**.
- 6 Click **Yes**.

Note: You can break port-to-port connections from the Device Manager, but you can break a device-to-device connections only from the Line Manager

To force a new connection to another device

- 1 Click the **Create Connection** button.

If a connection exists for the device, the existing connection is displayed.

- 2 Select **Another Device** from the list box.

- 3 Click **Next**.
- 4 Enter the device's domain name, IP address, or MAC address.
- 5 Click **Next**.
- 6 Select a port number from the list box.
- 7 Click **Next**.
- 8 If a connection exists for the other device, click **Next** to confirm the connection.

To force a new connection to a virtual device

- 1 Click the **Create Connection** button.
If a connection exists for the device, the existing connection is displayed.
- 2 Select **Virtual Device** from the list box.
- 3 Click **Next**.
- 4 Enter the number of the virtual device.
- 5 If no virtual device with that number exists, click **Yes** to create a new virtual device.

Changing Alarm Thresholds

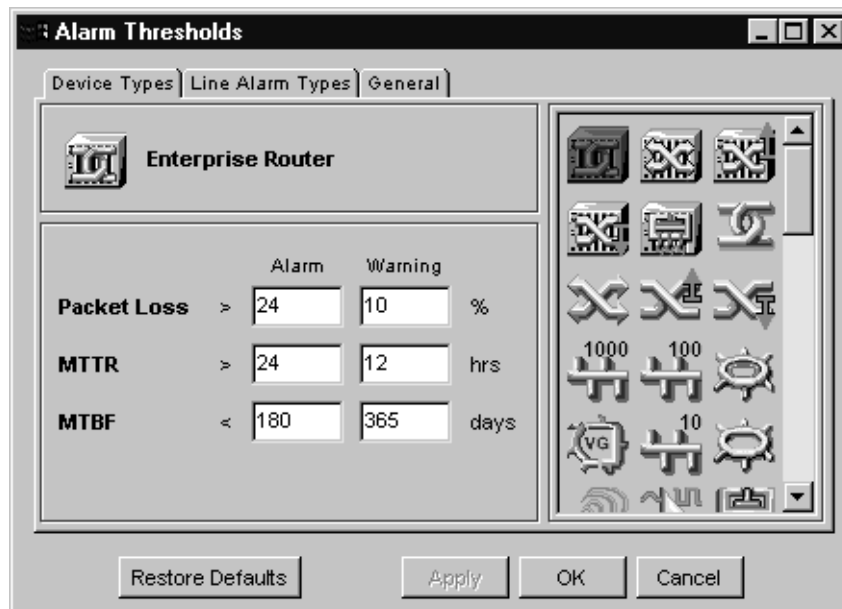
The Alarm Thresholds command lets you set alarm and warning levels for all the functions that Network Discovery monitors. Any changes to the Alarm Thresholds applies across all map configurations for all accounts. These are universal changes.

You can access the Alarm Thresholds menu from any map window. Click **Edit > Alarm Thresholds**.

Device Types

The Device Types tab lets you view and set alarm and warning thresholds on device types.

Figure 7-4: Alarm Thresholds (Device Types)



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

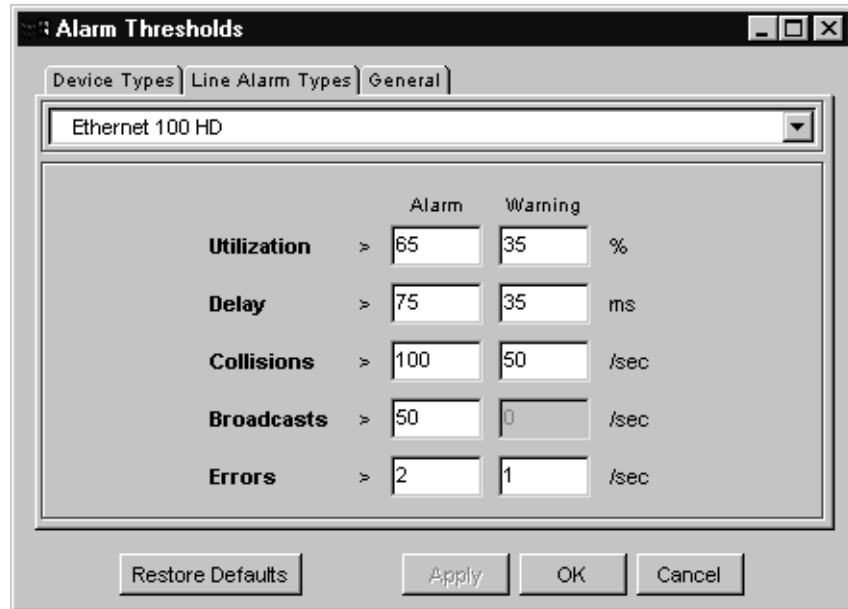
To change the Device Alarm Thresholds

- 1 Select a device type by clicking an icon from the scrolling panel.
- 2 Change a threshold by entering the desired value in the appropriate box.
- 3 Click Apply or OK.

Line Alarm Types

The Line Alarm Types tab enables the user to view and set alarm and warning thresholds based on line type.

Figure 7-5: Alarm Thresholds (Line Types)



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

To change the Line Alarm Thresholds

- 1 Select a line type with the list box.
- 2 Change a threshold level by entering the desired value in the appropriate box.
- 3 Click **Apply** or **OK**.

General

The General tab enables you to set:

- The number of days used to calculate the alarm and warning thresholds for NEWS (Network Early Warning System). NEWS predicts which devices will soon have a warning for packet loss or utilization. You can access NEWS from the Health Panel.
- The number of hours used to determine the Alarm condition for Changes. Changes identifies devices that have been added, moved, or have not been seen for a period of time. You can access Changes from the Health Panel.

Figure 7-6: Alarm Thresholds (General)

Alarm Thresholds

Device Types | Line Alarm Types | **General**

	Alarm	Warning	
Changes	< 6	0	hrs
NEWS	< 180	365	days

Restore Defaults Apply OK Cancel

8

Packaging Your Network

CHAPTER

You can group objects into “packages” so that the map is tidier and easier to understand.

No matter what type of account you have, you can package the network any way you want.

Topics in this chapter include:

- *How packaging works* on page 102
- *Changing the automatic packaging preferences* on page 107
- *You can request the creation of packages* on page 104
- *You can create your own multi-object packages* on page 105
- *Changing a package icon* on page 108

How packaging works

By packaging devices, you can reduce the size of the Network Map. You can package your network differently in each map configuration file.

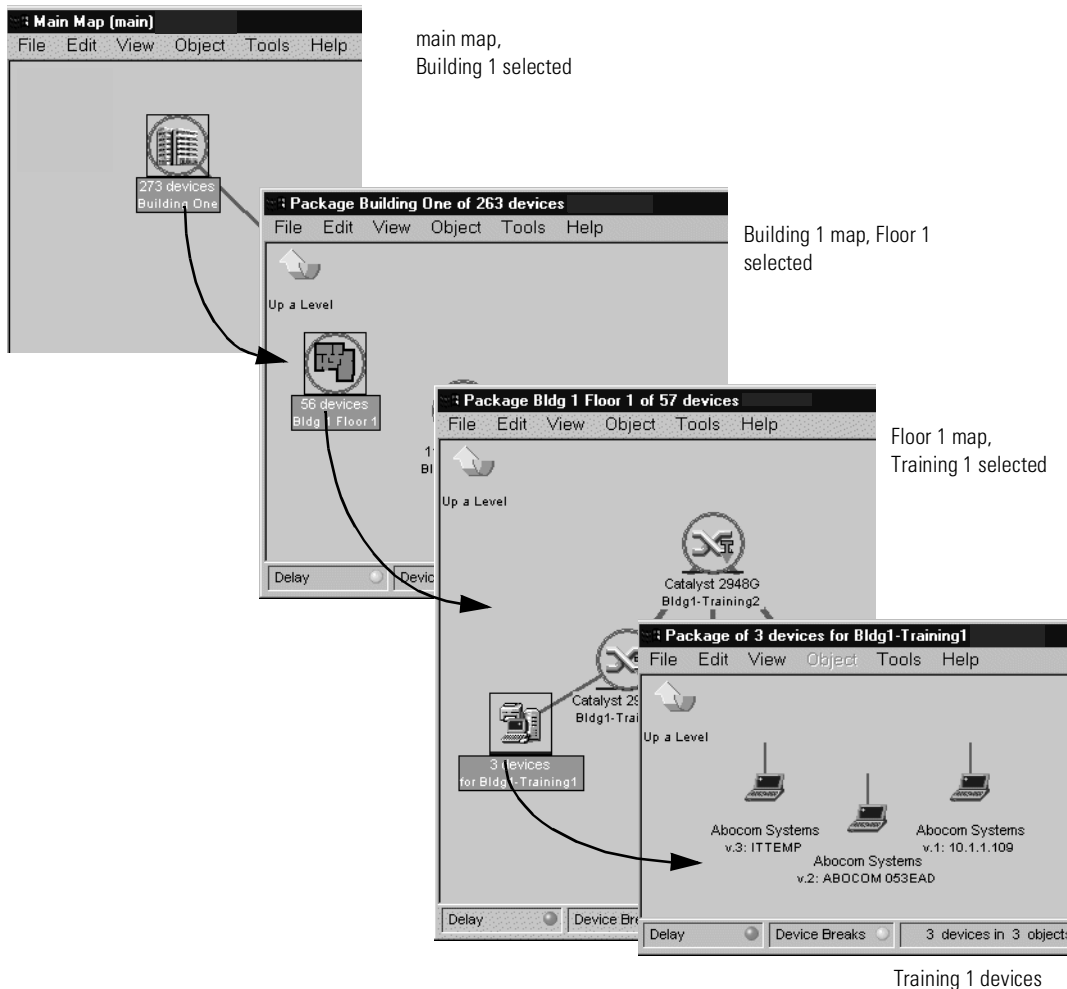
You can create packages to represent hierarchies, such as campuses, buildings, floors in buildings and so on. There are many package icons available to help you create the desired look and feel of the Network Map. For a description of the package icons, see the *Reference Manual*.

When you double-click a package icon, a separate window opens to reveal the contents of the package.

There are two types of packages: the type Network Discovery creates automatically (end node packages), and the type you can create yourself (multi-object packages).

One application of multi-object packaging is mapping the network at a physical location, such as a building. For example, in Figure 8-1, the main map contains a package for Building 1. Drilling down one level, the Building 1 map contains packages for floors within that building. Drilling down to the Floor 1 map, the network is broken down into its components, including individual devices and end node packages, such as Training 1. Training 1 could represent a room within Floor 1. Finally, you reach the devices for Training 1 within the end node package.

Figure 8-1: Location packages



Network Discovery creates end node packages automatically

An end node is defined as a device with only one connection. You may have devices in your network that have been physically modified, and may have more than one connection. A device with more than one connection is not included in an end node package (unless it is a telephone or a virtual device).

Network Discovery automatically creates end node packages, based on the major connectivity devices in your network. Connectivity devices (for example, routers or switches) will have other devices associated with them (for example, workstations). Network Discovery automatically packages the devices associated with that connectivity device.

These packages appear on your map with the label “X devices for Y” where X is the number of devices (this number is constantly updated as devices are added to or removed from the package) and Y is the name of the connectivity device.

Note: Network Discovery usually treats a telephone as an end-node, but it may see it as a connectivity device.

You can request the creation of packages

Network Discovery can create packages for you. This is a quick way to reduce the size of the Network Map. Network Discovery will create a package for each port of the device at the top of the network. Each package will contain the devices connected to that port.

To have Network Discovery create your multi-object packages for you

- 1 Select a map window.
- 2 From the **View** menu, click **Pack**.
You are asked to confirm the action.
- 3 Click **Pack**.

The **Pack** command does not lock your objects on the Network Map.

The **Pack** command does not delete any existing packages. However, the **Pack** command will remove any other layout changes you have made.

If you wish, you can open each package and click **Pack** again to continue packaging your network.

Multi-object packages can be created by the user. Network Discovery can create them with the **Pack** command, but if the packages are to be meaningful to you, it is best to create them yourself.

Note: Exception: While customizing your network, you may decide to use the **Unpack All** command. This command will destroy all the packages you have created. However, Network Discovery will automatically recreate all of the end node packages.

You can create your own multi-object packages

If you wish, you can create your own packages as well. Packages you create are called multi-object packages. How you package the Network Map will depend on how your network is connected, and on how you want to view the map. You are not, of course, changing the actual connectivity of any devices only how you view them on the map.

Note: Remember, you can create many different map configuration files, each with different packaging.

Here are three quick procedures that will show you how to create your own packages.

To create a new package with objects in it

- 1 Click an object icon, or select a group of objects.
- 2 From the **Object** menu, click **Package**.

To create a new package with objects in it

This method is handy for tidying up devices connected to a Logical View icon.

- 1 Right click an object that has dependent objects.
- 2 Select **Pack**.

The object will absorb any dependent object that:

- is not packaged
- is not locked
- does not have another connection.

To create a new package without any objects in it

- 1 From the **View** menu, click **Create Package**.
- 2 Add objects by dragging icons into the new package.

Note: You cannot open a New Package; it is empty.

Note: You can create one New Package in a window at a time.

Locked objects

If you have manually packaged your map configuration, you will see many icons with a blue line beneath them, if you have selected the “Underline locked objects option in **Edit > User Preferences**. The blue line indicates that the device has been manually packaged, meaning it has been put inside a package (**Package** command), promoted from a package (**Up a Level, Promote**), or has had its package removed (**Unpackage**).

Figure 8-2: Example of a Locked Device



When you manually package or unpackage an icon, you lock it into position. For example, if you take a workstation icon from a package and place the icon on the Network Map, that workstation icon will be locked there.

Network Discovery creates some automatic packages. Whenever you use the **Pack** or the **Unpack All** commands, Network Discovery will recreate end node packages automatically. To keep an end-node device (a device with a single connection), from being automatically included in an end-node package, you can either lock the device into another location or use the **Unlock** command.

To use the **Unlock** command

► **Object > Unlock**

Note: To see which objects have been locked, turn on **View locked objects**.

An icon you have moved yourself—into a place Network Discovery would not naturally have chosen—will have a blue line beneath it to indicate that it is locked.

Changing the automatic packaging preferences

Network Discovery packages similar end nodes. If you have an Administrator account, you can change whether or not each class of end nodes is packaged, or whether all classes are treated as one.

By default, whenever Network Discovery detects two or more end nodes of any classes, it creates a package to contain those objects. If it detects three or more objects of the same class (for example, workstations) it will create class-specific packages.

The defaults work well with most networks. You can change them to package the network in a particular way. In order to fully understand the possible scenarios, see *Automatic Packaging* on page 399 in the *Reference Manual*.

There are seven end node package types available:

- Workstations
- Servers
- Printers
- POS/ATM
- Controllers
- Unknown
- End Nodes

Note: The End Nodes package is a generic package type. If there are devices that do not fit the thresholds of another package type, those devices may fit into a generic End Node package. There are also three device icons native to this package type.

End node packaging settings do not affect your ability to create custom packages.

To create end node packages of a particular type

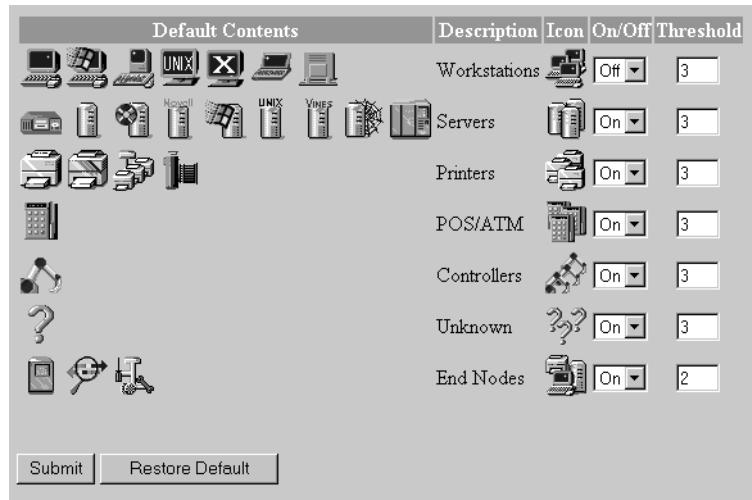
- 1 Click **Administration > Display preferences > Automatic packaging**.
- 2 For the package types you want to create, turn the package type On.
- 3 Select a threshold for each type of end node package.

To prevent a class of end nodes from being packaged, turn it Off.

To restore the defaults

- ▶ Click Restore Default.

Figure 8-3: Automatic Packaging preferences



Changing a package icon

To change a package icon

- 1 With the package selected, click **Object > Properties**.
- 2 In the Properties dialog, click an icon in the list box.
- 3 Click OK.

The object icon changes within the map window.

To reset the icon to the default chosen by Network Discovery

- 1 In the Properties dialog, click the “Use default icon” check box.
- 2 Click OK.

9 Organizing Map Configuration Files

CHAPTER

Network Discovery lets you save different map configuration files. Each of these map configurations contains your layout, icon titles, and packaging. You can save as many configurations as you want, so you can quickly change your view of the Network Map.

For example, you may want to concentrate on one particular building or campus. So, you create a map configuration that shows that campus, and all your important devices there. In another map configuration, you may want to see an overview of the entire network.

Topics in this chapter include:

- *The Prime configuration* on page 110
- *Starting a map configuration* on page 111
- *Saving a map configuration file* on page 111
- *Saving the Prime map configuration* on page 112
- *Opening a saved map configuration file* on page 112
- *Managing map configuration files* on page 113
- *Restoring the Prime map configuration* on page 115

The Prime configuration

The Prime configuration is a special configuration not associated with a particular account. As the owner of an Administrator account or an IT Manager account, you control the Prime map configuration. The Prime configuration can serve as a basis or starting point; people can copy it and make their own configurations.

Settings in the Prime configuration don't only affect the Network Map; they can affect other areas of Network Discovery such as Reports or Event filters.

Event filters are dependent on the device priorities as set in your Prime map configuration. If you make any changes to the Prime map configuration, you could affect your event filters. If you make any changes to your event filters, ensure that your Prime map configuration is set up properly. For more information on event filters, see *Setting up Event Filters* on page 129.

Saving your changes

Each account may save one or more named map configuration files. Each file contains information on the account's Network Map, and priorities, layout, packaging, and package icons and titles.

An account owner can use the different map configuration files for different purposes. For example, one configuration file could show the network geographically, and another configuration file could show the network by subnets.

An account may open a different configuration at any time. Once saved, this configuration becomes the “current” configuration and will be used for the next map session.

Note: Your current configuration is normally the one active when you exit the Network Map, but you can alter this with the **Manage Map Configurations** option.

Each account has the configuration files saved in a separate space. Therefore, each account may have a configuration named “test” without interfering with other accounts.

Starting a map configuration

Note: A new configuration will be labeled “Untitled” until you save it, at which time you are able to name the file.

To start a new map configuration

- ▶ From the File menu, click New.

Saving a map configuration file

Creating a specific configuration name enables you to see your configuration the next time you log in to the Network Map.

A configuration name must be 1–30 characters long. You can use the following characters:

- A through Z (upper case)
- a through z (lower case)
- 0 through 9 (numbers)
- underscore (_)
- hyphen (-)

Configuration names are case sensitive; “simple” and “Simple” are two different filenames.

To save a map configuration

- 1 From the **File** menu, click **Save As**.
- 2 Enter the new configuration name.
- 3 Click **OK**.

Autosave

Network Discovery provides an autosave capability for recovery purposes by saving the “current” configuration to a recovery file. Network Discovery will make an autosave file (within a time period ranging from 10 seconds to two minutes, depending on the changes made by the account). If a session ends abnormally, the recovery file will be used the next time you open a map.

When you next open a map, you will see the message “Restored configuration from autosave” to remind you that a recovery has occurred. In the event that Network Discovery uses the recovery file, the user still has the opportunity to discard the unsaved changes and re-open the configuration that represents the state of the last explicit save.

Note: Autosave will not overwrite your named configuration. When you respond “no” to the question “Do you want to save the changes?”, you are discarding the active changes and the autosave file. The autosave file is also discarded when you save a configuration.

Saving the Prime map configuration

The Prime map configuration is the default configuration for all accounts. Any account can open the Prime map configuration, but only admin and IT Manager accounts can change it. IT Employee and demo accounts must save their changes under a different file name.

To save the Prime map configuration

- 1 From the **File** menu, click **Save As Prime**.

A confirmation box appears, asking if you really want to save this configuration as the Prime configuration.

- 2 Click **Save As Prime**.

Opening a saved map configuration file

You can only open your own configuration files with this procedure. If you wish to use the configuration file of another account, you must first copy that file into your account.

Note: When you open a configuration file, all open package windows close. The Device Manager windows, Port Manager windows, Line Manager windows, Main Map, and Health Panel stay open.

To open a saved map configuration

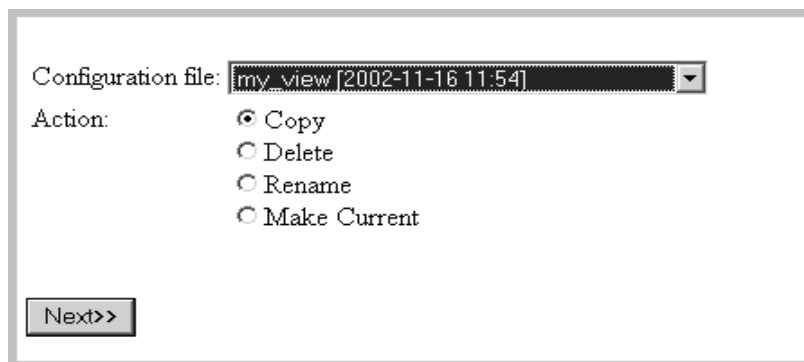
- 1 From the **File** menu, click **Open**.
- 2 Select the file name of the configuration you wish to use.
- 3 Click **OK**.

Managing map configuration files

This section is for any accounts, except demo. The demo account cannot perform any administration functions. The other three types of accounts can:

- copy map configuration files
- delete map configuration files
- rename map configuration files
- choose which map configuration file will be the one that opens first (Make current)

Figure 9-1: Managing map configurations



Note: Close your map before performing any of these procedures.

To reach the Administration menu, click the **Administration** button.

To copy a map configuration file

- 1 Click **Administration > My map configurations > Manage map configurations**.
- 2 Select a configuration file from the first pull-down list.
- 3 Select **Copy**.
- 4 Click **Next**.
- 5 Enter a name for the new configuration file.
- 6 Click **Finish**.

To delete a map configuration file

- 1 Click **Administration > My map configurations > Manage map configurations**.

- 2 Select a configuration file from the first pull-down list.
- 3 Select **Delete**.
- 4 Click **Next**.
- 5 Click **No** to delete the file.

To rename a configuration file

- 1 Click **Administration > My map configurations > Manage map configurations**.
- 2 Select a configuration file from the first pull-down list.
- 3 Select **Rename**.
- 4 Click **Next**.
- 5 Enter a name for the new configuration file.
- 6 Click **Finish**.

To choose which map configuration that will open first

The command, **Make Current**, makes a map file the first one you see when you open the Network Map.

- 1 Click **Administration > My map configurations > Manage map configurations**.
- 2 Select a configuration file from the first pull-down list.
- 3 Select **Make Current**.
- 4 Click **Next**.
- 5 Click **Yes** to make this your default map configuration.

Sharing map configuration files with other accounts

You can make it possible for other accounts to make copies of your files, but you cannot actually send a file. The procedure is simple and quick. First, you make sure that your account has its permissions set correctly. Next, the user with whom you want to share the file requests it.

To permit others to share your map configuration files

- 1 Click **Administration > My account administration > Modify properties**.
- 2 Click **Account Properties**.
- 3 Select “Yes” from the “Allow others to copy map configurations?” list box. (If “Yes” has already been selected, your task is complete.)

4 Click **Modify Properties**.

You have just permitted *all* users to copy *all* your map configuration files.

Figure 9-2: Allow others to copy your map configuration files

Click "Yes" to let others copy your map files

Account type:	IT Employee
Account capabilities:	Web Access: Yes
	MySQL ODBC Access: No
	ApE Access: None
	Shared directory Access: No
Name:	<input type="text"/>
Allow others to copy map configurations?	<input checked="" type="radio"/> Yes <input type="radio"/> No
<hr/>	
Append IP Address to device titles?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Make URLs visible?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Draw borders on tables in text mode?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Alternate colors in table rows?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Highlight table rows on mouse over?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Show navigation bar?	<input checked="" type="radio"/> Yes <input type="radio"/> No

What the other user must do

Note: The other user must not have a map session open.

- 1 Click **Administration > My map configurations > Copy map configurations**.
- 2 Select an account name (of the person whose file they want to copy) and click **Next**.
- 3 Select a configuration file and click **Next**.
- 4 Enter a name for the configuration file.
- 5 Click **Finish**.

The other user now has a copy of one of your map configuration files.

Restoring the Prime map configuration

This procedure enables you to restore the "Prime" configuration file from a backup.

Note: You will need this function only when you are told that the existing “Prime” configuration has become corrupt.

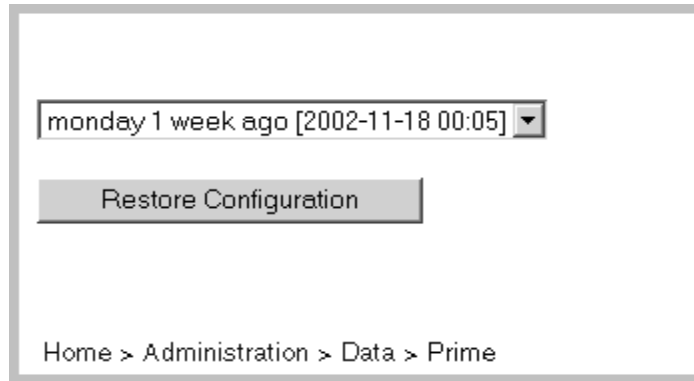
To restore the Prime map configuration

- 1 Click **Administration > Data management > Restore prime map configuration**.
- 2 Select a backup from the list box.

Note: The list box shows only those backups for which there is a Prime configuration.

- 3 Click **Restore Configuration**.

Figure 9-3: Restore the Prime map configuration



10 Setting up Paging

CHAPTER

This section is for Administrator accounts only.

You can configure Network Discovery to contact an account through an alphanumeric pager, by e-mail or through an SNMP trap or through all three. Then Network Discovery can tell the account about network problems or report about the success of a backup.

Topics in this chapter include:

- *Tasks not covered in this chapter* on page 118
- *Adding a new service provider* on page 119
- *Listing your service providers* on page 120
- *Testing your pager service provider* on page 121
- *Modifying modem properties* on page 122
- *Modifying account profiles* on page 123
- *Configuring event filters for paging* on page 124
- *Testing the pager address* on page 124
- *Testing the pager number* on page 125
- *Modifying information for a service provider* on page 125
- *Deleting a service provider* on page 127

Tasks *not* covered in this chapter

Installing and setting up an external modem or an SMTP server

You can set up paging to be through an external modem connected to the Peregrine appliance or through a Simple Mail Transport Protocol (SMTP) server. If you set up paging through the SMTP server, Network Discovery sends an e-mail to the pager service provider to forward.

If you choose to use an SMTP server, you do not need to install an external modem. It is easier to set up paging by e-mail on the SMTP server but you may not be paged, if part of your network, or your Internet Service Provider's network goes down.

If you choose to install an external modem, see the *Network Discovery Setup Guide* for recommendations on the type of external modem to acquire. For installation instructions, see the information supplied with the external modem.

Connect the external modem to a USB port on the Peregrine appliance, with reference to the server installation documentation that was included in the shipping box with your Peregrine appliance.

Entering the e-mail address

You should already have entered the Network Discovery Administrator e-mail address (**Administration > Appliance Management > Appliance administrator e-mail address**).

You need to enter the Network Discovery Administrator e-mail address for paging and for e-mail, even if you want another account to receive e-mail or pages.

If the Network Discovery Administrator e-mail address is not set properly, your pager will not work.

If you are using an SMTP server, you should already have entered the SMTP server (**Administration > Appliance Management > SMTP Server**)

(If you choose to install an external modem, you do not need to enter an SMTP server.)

Instructions for entering the Appliance administrator e-mail address and the SMTP server are in the *Setup Guide*.

Setting up event filters

- You will also need to set up your event filters (see *Setting up Event Filters* on page 129) but you can do that later.

Adding a new service provider

There are many pager service providers. If your system uses several pager service providers you will have to add all these providers to your list.

You can add the service name, data bits, parity, stop bits, baud rate, dialed number, protocol and description below. Contact your pager service provider for this information. You must enter data in all fields (except the description field; it is optional).

To add a pager service provider

- 1 Click **Administration > Pager service provider configuration > Add a service provider**.
- 2 Enter a service name.
Any upper case letters will be converted to lower case once the profile is created.
- 3 Select data bits from the list box.
- 4 Select parity from the list box.
- 5 Select stop bits from the list box.
- 6 Select a baud rate from the list box.
- 7 Enter a telephone number for the service provider.
Do not include a hyphen in the telephone number.
- 8 Select a protocol from the list box.
- 9 (optional) Enter a description of the service provider.
- 10 Select the enabled status from the list box.
- 11 Click **Add Data**.

Note: By default, profiles are not enabled. This means that accounts will not see the profiles.

Figure 10-1: Add a Service Provider

Service name

Data bits

Parity

Stop bits

Baud rate

Dialed number

Protocol

Description

Enabled

Home > Administration > Pager Service Providers > Add

Listing your service providers

You may want to verify that you have correctly input the information for your pager service provider.

To see a list of all of the pager service providers currently entered into Network Discovery:

- Click **Administration > Pager service provider configuration > List service providers**.

A list of all your pager service providers appears.

Figure 10-2: List Service Providers

Service Name	Data Bits	Parity	Stop Bits	Baud Rate	Dialed Number	Protocol	Enabled
<u>cantel</u>	8	Even	1	300	5551212	TAP	Yes
<u>test1</u>	8	Even	1	300	1234567	TAP	Yes
	Test 1						
<u>test2</u>	8	Even	1	300	1234567	TAP	Yes
	Test 2						

Home > Administration > Pager Service Providers > Listing Service Providers

Testing your pager service provider

This procedure sends a test message to your alphanumeric pager through the dialup service provider.

To select a service provider

- 1 Click **Administration > Pager service provider configuration > Test service provider**.
- 2 Select a service name from the list box.
- 3 Click **Test**.

To test the selected service provider

- 1 Enter a pager ID.
- 2 Click **Test Provider**.

If an error occurs and you do not receive the page, it could be because:

- There is no external modem connected to the Peregrine appliance
- The external modem connected to the Peregrine appliance is turned off
- Your pager is turned off
- There is incorrect pager data in the pager service provider profile
- The pager ID is incorrect
- There is no dial tone on the phone line being used

- Your service provider is having problems
- There are modem synchronization problems

Figure 10-3: Test pager service provider



Modifying modem properties

You can modify the modem initialization string and the dialing prefix.

- To determine the modem initialization string reference the AT command set for your particular modem. The default is L3&K0&M0. This should turn the speaker volume high, disable data compression and disable error control.
- The dial prefix may be any number of numerical digits. For example, dial 9 to get an external line. There is no default prefix. You can use commas to act as a pause. For example, “9,” would provide you access to the external line, and provide a pause before sending the rest of the number.

To modify modem properties

- 1 Click **Administration > Pager service provider configuration > Modem properties**.
- 2 Enter the modem initialization string and dial prefix in the text boxes.
- 3 Click **Modify Data**.

To return modem properties to their default settings

- 1 Click **Administration > Pager service provider configuration > Modem properties**.
- 2 Click **Default Values**.

Figure 10-4: Modify Modem Properties

Modem initialization string:

Dial prefix:

Home > Administration > Pager Service Providers > Modem

Modifying account profiles

Important: If the Network Discovery Administrator does not enter the correct pager information in an account's contact data, the owner of the account will not receive pages.

To modify an account profile

- 1 Click Administration > Account administration > Account contact data.
- 2 Select an account name from the pull-down list.
- 3 Click **Modify Properties**.
- 4 You can now modify any of the contact information.
- 5 Check to make sure the changes are correct.
- 6 Click **Modify Contact Data**.

To enable paging through an e-mail gateway

- ▶ Enter a pager address in the Pager e-mail address field.

To enable direct alphanumeric paging

- ▶ Enter a pager number.
- 1 Select a pager service provider from the list box.

Figure 10-5: Modify contact data



E-mail address:

Pager e-mail address:

Pager number:

Pager Service Provider:

Configuring event filters for paging

You can configure device and line event filters to determine who will be paged when events occur. For full details, see *Setting up Event Filters* on page 129.

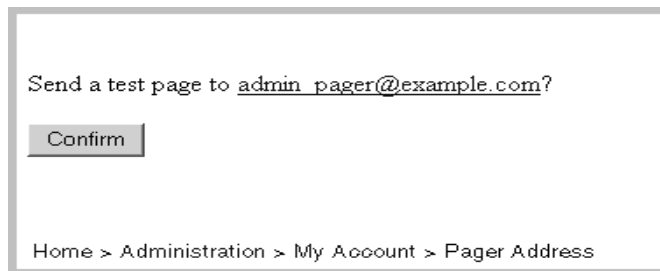
Testing the pager address

This will send an e-mail message to your pager, so that you can:

- test that you have entered your pager address correctly
- test that the Peregrine appliance has been configured to send e-mail

To test your pager address

- 1 Click **Administration > My account administration > Test pager address**.
- 2 To send an E-mail message to your pager, click **Confirm**.

Figure 10-6: Test pager address

Testing the pager number

This will send a test message to your alphanumeric pager through the dialup service provider.

Tests both that your pager is working and that the dialup service provider is configured correctly.

To test your pager number

- 1 Click **Administration > My account administration > Test pager number**.
- 2 To send a message to your pager, click **OK**.

Figure 10-7: Test pager number

Modifying information for a service provider

If there are changes to your pager service provider, you will want to update Network Discovery with the current information.

To select a profile

- 1 Click **Administration** > **Pager service provider configuration** > **Service provider properties**.
- 2 Select a profile from the list box.
Profiles are listed by description, not service name.
- 3 Click **Modify**.

To modify a profile

- 1 Select data bits from the list box.
- 2 Select parity from the list box.
- 3 Select stop bits from the list box.
- 4 Select a baud rate from the list box.
- 5 Enter a telephone number for the service provider.
Do not include a hyphen in the dialed number.
- 6 Select a protocol from the list box.
- 7 (optional) Enter a description of the service provider.
- 8 Select the enabled status from the list box.
- 9 Click **Modify**.

Figure 10-8: Modify a Service Provider

Service Name cantel

Data bits 8

Parity Even

Stop bits 1

Baud rate 300

Dialed number 5551212

Protocol TAP

Description CanTel, Toronto

Enabled Yes

Modify Data

Home > Administration > Pager Service Providers > Properties

Deleting a service provider

If you stop using a pager service provider, you will want to delete it from the Network Discovery database. Once deleted, the pager service provider data cannot be restored.

To delete a profile

- 1 Click **Administration > Pager service provider configuration > Delete a service provider**.
- 2 Select a profile from the list box.
Profiles are listed by description, not service name.
- 3 Click **Delete Service Provider**.
You are shown the profile you have requested.

Warning: This action cannot be undone.

You are asked to confirm the action.

- 4 Click **OK**.

11

Setting up Event Filters

CHAPTER

Setting up Event Filters is for Administrator accounts only.

You can configure Network Discovery to log events and to notify you when events occur. Network Discovery can notify you by e-mail, by pager, or by SNMP trap (or all three). For example, you can create an event filter to notify you when a particular device has a Break alarm.

Topics in this chapter include:

- *Interactions that affect Event Filters* on page 130
- *What is an Event Filter?* on page 131
- *Preparing Network Discovery for Event Filters* on page 132
- *Examples of common Event Filters* on page 133
- *Modifying a filter* on page 140
- *Deleting a filter* on page 142
- *Listing Event Filters* on page 142
- *Resetting to Defaults* on page 143

Interactions that affect Event Filters

The most important thing to remember about event filters is that they rely on the device priorities as set in the Prime map configuration. The Prime map configuration is controlled by Administrator and IT Manager accounts. In order for your event filters to work properly, you must make sure your Prime map configuration is set up properly. Also, when you are using Network Discovery to respond to notifications (e-mail, pager messages), make sure you access the Prime map configuration.

Be very careful when setting up your event filters. Many factors contribute to making your event filters work effectively. Make sure you complete all of the tasks in this chapter. If you skip any of these tasks, or if you do any of them incorrectly, your event filters may not work.

If you are not familiar with the following concepts, read the appropriate sections of this *Network Discovery User Guide*, and also read the appropriate sections of the *Reference Manual*.

Table 11-1: References to interactions that affect Event Filters

Concept	Commands and where to get more information
E-mail Issues	
Set up your SMTP server	Administration > Appliance Management > SMTP Server See the <i>Network Discovery Network Discovery Setup Guide</i>
Events Issues	
Understand the types of events recorded by Network Discovery	<i>The Events Browser</i> on page 70 in <i>A Tour: Toolbar, Health Panel, Network Map</i> on page 45.
Hardware Issues	
Set up and test your pager equipment (hardware and software)	<i>Setting up Paging</i> on page 117
Account Issues	
Set up account contact information	Administration > Account administration > Account properties <i>Modifying account contact information</i> on page 30

Concept	Commands and where to get more information
Set up your Network Discovery Administrator e-mail address	Administration > Appliance Management > Administrator e-mail address See the <i>Network Discovery Setup Guide</i>
Network Map Issues	
Change device priorities	<i>Changing the priority of a device</i> on page 90
Change device icons (which may change the default device priority)	<i>Changing a device icon</i> on page 91
Changing alarm thresholds	<i>Changing Alarm Thresholds</i> on page 96
Save the Prime map configuration	<i>Organizing Map Configuration Files</i> on page 109

Event filters are an advanced option. You have the power to send pager and e-mail messages whenever a device changes state. This means that the potential exists to send several pager and e-mail messages for the same event on the same device.

You must make sure you are setting up the event filters properly, to avoid excessive notification, or notification on the wrong devices, or no notification at all.

If you have read this section and believe you have set up all the components properly, and your events filters are not working properly, call Customer Support.

What is an Event Filter?

Event filters control what network events will be recorded as they occur. Once the events are recorded, you can find out about them in several ways.

Network Discovery can:

- send an e-mail
- send an alphanumeric page
- send an alphanumeric page by means of an e-mail gateway
- send an SNMP trap to another network management system
- log the event in the Network Discovery events database for you to view with the Events Browser

Network Discovery has two kinds of event filters: line filters and device filters. There are five default filters available.

Table 11-2: Default Event Filters

Default Event Filter	Description
email-admin-device	Send e-mail to the “admin” account ^a when a device of priority 6 breaks.
email-admin-line	Send e-mail to the “admin” account ^a when a line of priority 6 breaks.
log-events-device	Log all events that occur on devices of priority 3, 4, 5, or 6.
log-events-line	Log all events that occur on lines of priority 3, 4, 5, or 6.
log-add-delete	Log all add and delete events.

^aThe “admin” account is the default Administrator account. If you have changed the name of this Administrator account when initially setting up Network Discovery, you should have changed these default event filters.

Preparing Network Discovery for Event Filters

In order to have event filters work properly, you must have several components set up.

- Make sure the following is set up in Network Discovery:
 - Network Discovery Administrator e-mail address
 - SMTP server
 - SNMP traps setup (only if you plan to use SNMP traps)
 - Pager setup (hardware installation and pager service provider information)
- For accounts who are going to receive e-mail or pager messages:
 - Make sure their accounts are set up with proper e-mail addresses and pager numbers.
 - Test their e-mail addresses and pager numbers to make sure they are working.
- Make sure the Prime configuration is set up with the proper device priorities.
- Set up the proper alarm and warning thresholds.

Once you know how to use all of these components together, you are ready to set up your event filters.

Examples of common Event Filters

There are many ways to set up event filters. Sometimes, it is difficult to understand all the possible implications. There have been occasions where users have been paged several times a day for devices that are not broken or overutilized.

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

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

Example 1: Notification when a core device breaks

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

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

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

To set up the Administrator account

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

To set up the Prime map configuration

- 1 Open the Prime map configuration.
- 2 Find your core device and select it.
- 3 Click **Object > Properties**.
- 4 Make this device priority 6.

Warning: Changing this device type to priority 6, and creating an event filter for it, means that you will be notified for all devices of this type and this priority.

- 5 Click **Apply**.
- 6 Click **OK**.
- 7 Save your Prime map configuration by clicking **File > Save As Prime**.

You have now saved your Prime map configuration with your core device as priority 6.

To set up the event filter

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

Field	Enter:
Name (create a name for the filter)	core_device_broken
Description	Page administrator when core device breaks
Device Event Category	Breaks
Priority	6
Transitions	OK > Alarm, Warn > Alarm
Device Type	ATM Switch
Alphanumeric Page	Select the Administrator account
Log	Select "On" if you want the event logged

Note: The event will only be logged once, even if it is caught by more than one event filter. If you have not deleted or changed the default log_events_device filter, it will already be logging events on devices of priority 3,4,5, or 6.

3 Click Add Filter.

Figure 11-1: Example of a Device Event Filter

Name:

Description:

Selection Criteria

Device Event Category:

Priority:

Transitions:

Device Type:

IPv4 Range: Add by interval Add by subnet

Starting IPv4 Address: IPv4 Address:

Ending IPv4 Address: Netmask:

Added IP ranges: [No seeds to delete.]

Notification

E-mail:

Alphanumeric Page:

Alphanumeric Page (via e-mail gateway):

SNMP Trap:

Log: Off On

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

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

To set up the Administrator account

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

To set up the Prime map configuration

- 1 Open the Prime map configuration.
 - 2 Find your Router and select it.
 - 3 Click **Object > Properties**.
 - 4 Make this device priority 6.
 - 5 Click **Apply**.
 - 6 Click **OK**.
- If you want to set this up for several routers, then repeat these steps for each router.
- 7 Set the Packet Loss thresholds by clicking **Edit > Alarm Thresholds**.
 - 8 Click **Apply**.
 - 9 Click **OK**.
 - 10 Save your Prime map configuration by clicking **File > Save As Prime**.

You have now saved your Prime map configuration with your Router device as priority 6.

To set up the Event Filter

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

Field	Enter:
Name (create a name for the filter)	routers_dropping_traffic
Description	E-mail me when routers are dropping a lot of traffic
Device Event Category	Packet Loss
Priority	6
Transitions	OK > Alarm, OK > Warn, Warn > Alarm
Device Type	Router
E-mail	select the Administrator account
Log	select "On" if you want the event logged

3 Click Add Filter.

Figure 11-2: Second Example of a Device Event Filter

Name:

Description:

Selection Criteria

Device Event Category:

Priority:

Transitions:

Device Type:

IPv4 Range Add by interval Add by subnet

Starting IPv4 Address: IPv4 Address:

Ending IPv4 Address: Netmask:

Added IP ranges: [No seeds to delete.]

Notification

E-mail:

Alphanumeric Page:

Alphanumeric Page (via e-mail gateway):

SNMP Trap:

Log: Off On

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

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

To set up the Administrator account

- 1 Click **Administration > Account administration > Account contact data.**

- 2 Select the Administrator account that you want to change.
- 3 Click **Modify Properties**.
- 4 Enter the correct e-mail address.
- 5 Click **Modify Contact Data**.

To set up the Prime map configuration

- 1 Open the Prime map configuration.
- 2 Find your server and select it.
- 3 Click **Object > Properties**.
- 4 Make this Server priority 6.

Lines get their priority from the highest priority devices they connect. By making this device a priority 6, the lines attached to it are automatically a priority 6.

Warning: Changing this device type to priority 6, and creating an event filter for it, means that you will be notified for all devices of this type and this priority.

- 5 Click **Apply**.
- 6 Click **OK**.
- If you want to be paged for several servers, repeat steps 2-6 for each server.
- 7 Set the Device Alarm thresholds by clicking **Edit > Alarm Thresholds**.
- 8 Set the Line Alarm thresholds by clicking **Edit > Alarm Thresholds**.
- 9 Click **Apply**.
- 10 Click **OK**.
- 11 Save your Prime map configuration by clicking **File > Save As Prime**.

You have now saved your Prime map configuration with your server as priority 6.

To set up the Event Filter

- 1 Click **Administration > Event filter configuration > Add a line filter**.

2 Enter the event filter information as it appears in this table:

Field	Enter:
Name (create a name for the filter)	server_delays
Description	E-mail me when server lines have Delay warnings or alarms
Line Event Category	Delays
Priority	6
Transitions	OK > Alarm, OK > Warn, Warn > Alarm
Device Type	Server
Line Alarm Type	Ethernet 10< HD
E-mail	select the Administrator account
Log	select "On" if you want the event logged

3 Click Add Filter.

Figure 11-3: Example of a Line Event Filter

Name:

Description:

Selection Criteria

Line Event Category:

Priority:

Transitions:

Device Type:

Line Alarm Type:

IPv4 Range Add by interval Add by subnet

Starting IPv4 Address: IPv4 Address:

Ending IPv4 Address: Netmask:

Added IP ranges: [No seeds to delete.]

Notification

E-mail:

Alphanumeric Page:

Alphanumeric Page (via e-mail gateway):

SNMP Trap:

Log: Off On

Modifying a filter

To select a filter to modify

- 1 Click Administration > Event filter configuration > Modify a filter.
- 2 Select an event filter from the pull-down list.
- 3 Click Modify Filter.

To edit the description of the filter.

When using Selection Criteria list boxes, you can select multiple options.

Windows users: Use the Shift and Control keys in combination with clicking the mouse.

- 1 Select one or more options from the Event Category list box.
- 2 Select one or more options from the Priority list box.
- 3 Select one or more options from the Transitions list box.
- 4 Select one or more options from the Device Type list box.

Note: These selection criteria apply to all notifications.

You select by device type name. In the list, both icon and device type name appear.

To enter the IPv4 range

- 1 Click **Add by interval** and enter the starting and ending IPv4 addresses or click **Add by subnet** and enter the IPv4 address and netmask.
- 2 Click **Add IPv4 Range**.

Note: Use primary IPv4 addresses. To find a device's primary IPv4 address, look at the top of the Device Manager.

To select notification

- 1 Select the appropriate notification for the event filter:
 - E-mail
 - Alphanumeric Page
 - Alphanumeric Page (through e-mail gateway)
 - SNMP Trap
 - Log

To modify filter

- ▶ Click **Modify Filter**.

Note: Network Discovery does not check to see if the user has provided the appropriate contact data.

Deleting a filter

To delete an event filter

- 1 Click **Administration > Event filter configuration > Delete a filter.**
- 2 Select a filter name from the list box.
Profiles are listed by name.
- 3 Click **Delete Filter.**
- 4 Click **Confirm.**

Listing Event Filters

The filter names are hyperlinked. Clicking the hyperlinks will take you to the *Modifying a filter* page for that filter.

To list filters

- 1 Click **Administration > Event filter configuration > List filters.**
- 2 Click a filter name hyperlink.

Figure 11-4: List Event Filters

Device Event Filters							
Name	Device Event Category	Priority	Transitions	Device Type	IP Range	Notification	
email-system-device	Breaks	6	All	All		Send email to account 'system'	
Send email to system on priority 6 device break events.							
log-add-delete	Adds Deletes	All	All	All		Record event in events log	
Log Add Delete							
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-system-line	Breaks	6	All	All	All		Send email to account 'system'
Send email to system 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.							
server_delays	Delays	6	<input type="radio"/> OK -> Warn <input checked="" type="radio"/> OK -> Alarm <input type="radio"/> Warn -> Alarm	Server	4		Send email to account 'admin'
E-mail me when server lines have Delay warnings or alarms							

Home > Administration > Event Filters > List

Resetting to Defaults

To reset to default filters

Warning: This action cannot be undone.

- 1 Click **Administration > Event filter configuration > Reset to defaults**.
- 2 Click **Reset to Defaults**.

12

Locating Network Problems

CHAPTER

There are many ways to find network problems with Network Discovery. You can use the Network Map, the Health Panel, the Events Browser, the Reports, the Device Manager, the Port Manager and the Attribute Manager. All of these features will help you find trends and problem areas of your network. However, they all take a certain amount of analysis to locate the source of the problem.

Topics in this chapter include:

- *Finding the problem by means of the Service Analyzer on page 146*
- *Using the Network Map and the managers on page 147*
- *Checking network events with the Events Browser on page 149*
- *Drill down with the Device Manager on page 150*
- *Drill down with the Line Manager on page 153*
- *Drill down with the Port Manager on page 153*
- *The Attribute Manager on page 155.*
- *Sample troubleshooting scenarios on page 156*

Finding the problem by means of the Service Analyzer

“I can’t print” or “E-mail is down”

As a network administrator, two of the most common problems you hear from users are “I can’t print,” and “E-mail is down.” The users do not necessarily know where the problem might be, but they know something is wrong.

If you are receiving complaints from users, you need to find the source of the problem quickly. You can use the Service Analyzer. You will still need to check statistics, and investigate the Device Manager and Port Manager, but the Service Analyzer will give you a visual indication of where the problem is between two of your network devices.

To use the Service Analyzer to find the problem

- 1 On the Network Discovery Toolbar, click the **Service Analyzer** button.

A screen appears asking you to enter the IP addresses of the devices at either ends of the path you want to check.

- 2 Enter the IP addresses.
- 3 Click **Analyze**.

A screen appears showing the entire path between the two network devices. Alarmed devices appear with a red background. Alarmed lines appear red as well.

You can use the pull-down list to check the connection statistics between all the devices in the line. This helps you determine the problem, and fix it quickly.

Clicking the lines opens Line Manager sessions. Clicking the devices opens Device Manager sessions.

You can drill down to Service Level and Traffic Level graphs to analyze the data from connection to connection.

Once you have found the problem

Once you have located a network problem with the Service Analyzer tool, or through the Network Map, there are several ways to find out specific details.

This section gives a brief overview of how to locate and handle network problems by means of the:

- Device Manager
- Port Manager
- Attribute Manager
- Line Manager
- Events Browser.

Your company will have its own methods and procedures for dealing with the device, port, and line problems Network Discovery finds.

This section also offers two sample troubleshooting scenarios to demonstrate the different features in Network Discovery.

Using the Network Map and the managers

Start with the Network Map and Health Panel. By clicking any of the fault category buttons, you can instantly see all the current alarms and warnings on your network. From the Network Map, you can drill down to Device Manager, Port Manager, and Line Manager sessions to further evaluate the alarms and warnings.

Note: Events listed on the Health Panel are subject to the selected minimum priority. This is not the case with the Device Manager. For example, you may look at a Device Manager for a workstation (priority 1) and see that it has a device break alarm. This alarm will not have been listed on the Health Panel.

For details of information available from the Device Manager, Port Manager, and Line Manager, see the *Reference Manual*.

Start with the Network Map and Health Panel

Using the Network Map and Health Panel, you can quickly locate all alarms and warnings in your network. The Health Panel updates all alarm information in real time, so you will see a problem as soon as Network Discovery knows about it.

If you have a device alarm or warning, you will want to view the Device Manager. Double-click on the device, then see *Drill down with the Device Manager* on page 150.

If you have a line alarm or warning, you will want to view the Line Manager, and perhaps the Port Manager. Double-click on the line, then see *Drill down with the Line Manager* on page 153.

Using the Health Panel Reports

You can access recorded Device Faults, Line Faults, and Metrics reports by:

- clicking the column of reports buttons on the Health Panel
- selecting the **Health Panel Reports** command in the **Tools** menu

Do not confuse these reports with the network reports available from the Network Discovery Toolbar, which is also available from the **Reports** command in the **Tools** menu.

Each Health Panel report provides one row of data for each device that is reporting an alarm or warning. Clicking the device title opens a Device Manager. In the case of the Line Faults report, clicking the Port Index opens a Port Manager.

In the case of Line Faults, the report lists the IP address of the device, then the index to which the line is connected, and whether the traffic is incoming or outgoing. The line speed is also reported unless the line is reported to be broken. In that case, the time of the break will be reported.

If there are no alarms or warnings for a category button, then a window appears confirming that there is no data for that report. The message begins “No devices of priority \geq X have...” where X stands for the minimum priority specified in the **Priority** pull-down list (if the priority is 1–6).

Checking network events with the Events Browser

Use the Health Panel to view *current* states (Alarms, Warnings, OK) on the Network Map. To see states that are over and have disappeared, use the Events Browser.

The Events Browser will help you to track events that may be intermittent (that is, events that have occurred repeatedly, perhaps for only a short duration each time).

To access the Events Browser:

- ▶ On the main Toolbar click the **Events Browser** button.
OR
- ▶ From the Home page, click **Events Browser**.
OR
- ▶ From a Network Map window or from the Health Panel, click **Tools > Events Browser**.

By default, the Events Browser displays the 20 most recent events. You can use the first two buttons, (**Older** and **Newer**) to view more events. You can also move forward or back by typing a new date in the text box.

Once the Events Browser window is open, it does not update as new events occur.

Note: The Events Browser is subject to the limitations of the event filters, which in turn use the priorities from the Prime configuration. The Health Panel is not subject to any such filter. For more information, see *Setting up Event Filters* on page 129 or *Organizing Map Configuration Files* on page 109.

Note: If you are using Peregrine's Express Inventory, the WMI collector, you will notice a lot of "Add" events when scanned devices are added to the database. These devices will not have any other events associated with them because their data is not updated regularly.










Drill down with the Device Manager








The Device Manager provides you with detailed information about a specific device.

Device Manager panels





The Device Manager is split into several panels. Typically, you will not need to use many of these panels. However, there may be occasions when you or Network Discovery Customer Support need to access details the panels provide.

Table 12-1: Device Manager Panels

Icon	Button name	Description
	Configuration	Provides an overview of the device configuration, including any exceptions.
	State	Provides a summary of current device statistics.
	Statistics	Provides a second toolbar to view statistics in a variety of forms, or to export the statistics. Not all statistics are available for all devices. Only available statistics appear in the list box.
	Ports	Lists ports for this device and summarizes the information available for them. This panel lists Utilization Status, Utilization In and Out, a description of how the port is utilized and the rate. Provides a way to start the Port Manager. (the Port Manager gives a detailed look at one specific port.)
	Events	Provides a second toolbar to list all events that occurred to the device or the device's ports over a specified period.
	Diagnosis	Display information about the current state of the device that can be helpful in diagnosing internal problems.
	Locate	Highlights the location of the device on a map window.
	Service Analyzer	Opens a Service Analyzer session to show you the connection between this device and another device in your network.
	Manage	Will connect you to an external element management system. You must have set this up in Administration > Display preferences > Element management URL .

Icon	Button name	Description
	Browse MIB	Opens the MIB Browser to allow the user to view the device's SNMP MIB.
	View Scan Data	If you are using Peregrine's Express Inventory, the WMI collector, this panel allows you to see data from scan files. (Only available in a Device Manager for a scanned device.)
	Web	Attempts to open a web browser window for this device.
	Telnet	Attempts to open a Telnet session. Many network devices provide Telnet as a means to set up and configure the device.
	Update Model	Puts this device at the top of the device modeler's queue.
	Purge Device	An Administrator account can remove a device from the Network Map. See "Purge" in the <i>Reference Manual</i> .
	Properties	Modifies the properties of an object. Properties affect an object's appearance, priority, and placement within a map window.

Buttons on the Diagnosis Panel

	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.
	Traceroute	<p>Displays the path that data takes to get from the Peregrine appliance to the selected device by listing the gateway devices associate 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 will be hyperlinked to a Device Manager.</p> <p>Traceroute helps you to understand where on the network problems are occurring. It is often used after IP Ping has been used to confirm the existence of a device.</p>
	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.
	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.

Checking a device with the Device Manager

If the device is not providing data, try to ping it. There is a button for Ping in the Diagnostics panel. If there is no ping response, the device is likely broken, or may have been removed from the network. If the device icon has a gray background, Network Discovery has not seen the device for more than 24 hours.

Note: Scanned-only devices do not show a gray background.

If you suspect this might be a port problem, check the Ports panel. The Ports panel lists all the ports on this device and gives some detail. It will also link you to a Port Manager for each port to investigate further.

Check any of the following panels in the Device Manager. Depending on the problem with the device, any of these panels can help you determine the cause of any alarms or warnings.

- Check the Configuration panel.

The Configuration panel provides some very basic information about the device. There is a series of signal lights indicating the type of alarm and warnings currently active on the device. You can also see where this device is physically located (System Location), who is in charge of the device (System Contact). This information could help you track down the problem, and possibly who might be able to fix it.

- Check the State panel.

The State panel shows you Attributes of the device. You can click an Attribute to open the Attribute Manager for more information about a specific problem, including alarm and warning thresholds.

- Check the Statistics panel.

Check statistics graphs to inspect recent activity on the device. You may find a particular time when the device has experienced heavy traffic or other problems.

- Check the Events panel.

The Events panel is much like the Events Browser, but shows only events for this specific device.

Accessing the device

If the device is capable, you can access the device directly through one of the following:

- MIB Browser session
- Web session
- Telnet session
- Element Manager

Once you establish a session, you can configure the device. This enables you to address any problems arising from an improperly configured device. See *Example 2: Collision* on page 158.

Drill down with the Line Manager

To open a Line Manager double-click the line. The Line Manager shows you the connections at either end of the line. If one of the devices or ports is alarmed, you can check the port with the Port Manager, and the device with the Device Manager.

The Line Manager has a single panel called the “About” panel. The About panel displays statistics for ports on both sides of a connection. The port or device that provided the link to the Line Manager appears on the left side of the panel.












The Line Manager also has a Break Connection button. An Administrator or IT manager account can break the connection if Network Discovery has made incorrect assumptions about connectivity.



Drill down with the Port Manager

You can access the Port Manager through the Device Manager or Line Manager. You can evaluate the selected port, and change its properties through the many Port Manager panels.

Port Manager panels

Note: If necessary, an Administrator or IT Manager account can use the Interface Rate, Interface Type, Alarm Type, Duplex Mode, and Connection buttons to change the way Network Discovery perceives a connection. Contact Peregrine Systems Customer Support before you use the Create Connection button. Peregrine Systems Customer Support will help you diagnose why Network Discovery can't make the right connections on its own. (If you do break a connection, and Network Discovery still perceives the connection as legitimate, the connection will come back.)

Icon	Button name	Description
	Configuration	Identifies a port and presents an overview of the port's identity and status.
	State	Provides a summary of current port statistics.
	Diagnosis	Display information about the current state of the device that can be helpful in diagnosing problems.
	Statistics	Provides a second toolbar to view statistics in a variety of forms, or to export the statistics. Not all statistics are available for all ports. Only available statistics appear in the list box. Inbound and outbound data is displayed for most statistics.
	Events	Provides a second toolbar to list all events that occurred to the device's ports over a specified period.
	Locate	Highlights the location of the device on a map window.
	Interface Rate	Sets speed for a line.
	Interface Type	Sets the media type used for the line.
	Alarm Type	Sets the alarm type for the connection. The alarm type is normally associated with the interface type, but may be changed independently.
	Duplex Mode	Sets the duplex to full or half. Full duplex allows for two-way communication over a line; half duplex permits only one-way communication.
	Purge Port	Removes the port from the device's model as created by Network Discovery. You can purge a port, when a connection has been removed from the network and you want the Network Map to reflect the change immediately.

Icon	Button name	Description
	Create Connection	Creates a connection. You can force a connection to a device or to a virtual device. Connections changes take effect at the end of the current sampling period.
	Break Connection	Breaks an existing connection or forces a new connection. Forcing a new connection will first break any existing connection. You can force a connection to a device or to a virtual device. Connections changes take effect at the end of the current sampling period.

Check ports with the Port Manager

- Check the Configuration panel.

The Configuration panel provides some very basic information about the port. There is a series of signal lights indicating the type of alarm and warnings currently active on the port.

- Check the Diagnosis panel.

You can see the alarm thresholds, which can help you gauge the depth of the problem.

- Check the Statistics panel.

Check statistics graphs to inspect recent activity on the port. You may find a particular time when the port has experienced heavy traffic or other problems.

- Check the Events panel.

The Events panel is much like the Events Browser, but shows only events for this specific port.

The Attribute Manager






The Attribute Manager gives you the detailed history of an attribute associated with a device or a port.

The Attribute Manager also enables you to change the state of an attribute, and to change the way Network Discovery perceives an attribute.

To open the Attribute Manager

- ▶ Click an attribute hyperlink from:

- the Device Manager State panel
- the Line Manager State panel
- the Line Manager About panel.

Icon	Button name	Description
	Configuration	Identifies an attribute and presents details of its most recently observed state.
	Statistics	Provides a second toolbar to view statistics in a variety of forms, or to export the statistics. Not all statistics are available for all ports. Only available statistics appear in the list box. Inbound and outbound data is displayed for most statistics.
	Locate	Highlights the location of the device on a map window.
	Manage	Offers the options available for the attribute
	Purge Attribute	Removes the port from the device's model as created by Network Discovery. You can purge a port, when a connection has been removed from the network and you want the Network Map to reflect the change immediately.

Sample troubleshooting scenarios

In troubleshooting, the possible methods of attack are innumerable. The procedures will depend on the size and layout of your network, your company standards and methods, as well as the types of alarms and warnings appearing in your network. If you have exhausted your internal resources, call Network Discovery Customer Support for more help.

The two examples listed here are common network problems. The troubleshooting methods outlined here are only suggestions, which may or may not completely guide you to a solution.

Example 1: Device Break

The Health Panel shows one Device Break alarm. You select the Device Breaks button. The icon for the broken device is surrounded by a ring in the alarm color (red by default). The first thing you will wish to do is check the device's current behavior.

When you double-click the icon, you go to the Device Manager. Click the Ports button, and see a list of ports on this device. Look for ports with an alarmed Link Status signal light, or for ports with an alarmed Breaks signal light.

Examine one of the traffic counters such as bytes, frames, or broadcasts. If these values are 0 (zero), no traffic is moving in or out of the device. If these values are in parentheses (), the values are from an earlier poll cycle, indicating that no recent data is available.

You may now wish to ping the device. If there is no response from the device, you will need to implement your company's standard troubleshooting procedure, which might be:

- To begin a physical check of the device and its cables: go to the Configuration panel, and check System Location to find out where the device is located.
- To notify your network administrator: go to the Configuration panel, and check System Contact to find out who is responsible for the device.

If the device responds to the ping, you may want to try Traceroute or the Service Analyzer to see if another device is preventing traffic from reaching the device. You may also want to try SNMP ping, to see if the device's SNMP agent is still operational.

Once you have determined the device's current behavior, you may wish to check the recent past of the device. Go the Device Manager Diagnosis panel. In the State panel, you will see a row for "Break", which tells you how long Network Discovery believes the device has been broken, and the probable cause of the break.

If the probable cause of the break is "line break", go to the Line Manager. One way to do this is to go the Device Manager Ports Summary or Ports Statistics panel, and click on the [line] hyperlink for any port that seems to be handling traffic of 0. Alternately, instead of clicking on [line], click on the port index, which will take you the Port Manager.

Once in the Port Manager, go the Ports Statistics panel, where you will see the current statistics for the port. These values should help you confirm the working status of the port.

You may also wish to check the main diagnostic table for “Last seen”, to find out exactly when Network Discovery confirmed the existence and operation of the device.

Having established the recent past of a device, you may wish to consider the more distant past. You may wish to know if this device has a history of breaking. Go to the Statistics panel, and select Breaks from the list box. You can select various periods of time from the second list box, which gives you the ability to get an quick graphic overview of the device's history.

Alternately, go to the Events panel, and select Device Breaks from the list box.

Example 2: Collision

The Health Panel tells you that there is one Collision alarm. Select the Collisions button. A line between two devices (a switch and another device) is drawn in the alarm color. When you double-click the line, you will be taken to the Line Manager.

The Line Manager shows the devices and ports on each side of the line, and includes the port properties for each: interface type, interface speed, and duplex. You notice that although each port is of the same interface type and speed, the duplex for the switch is half, and the duplex for the other device is full. The collisions are being caused by a simple configuration problem.

You can easily configure the device from within Network Discovery. From the Line Manager, click the hyperlink for the switch, and you will be taken to the Device Manager. From here, you can establish an interactive session with the switch: you can use the MIB Browser to change a MIB parameter to change the port from half duplex to full, or telnet to the switch and set the port's duplex from the command line. It all depends on what type of interaction each device supports.

Note that the solution is to reconfigure the port, not simply change the way Network Discovery perceives the port. The Port Manager also enables you to adjust duplex, but because you are merely adjusting the perception and not the reality, the five center buttons of the Port Manager are intended for final efforts only. That's why these buttons are restricted to Administrator and IT manager accounts only.

13 Adding, Removing, and Replacing CHAPTER Devices

There will be many situations when you are adding, removing, or replacing devices in your network. You will have to take precautions when performing these activities, such as making sure all devices have unique IP and MAC addresses.

Topics included in this chapter are:

- *The importance of unique IP addresses* on page 160
- *Removing a device* on page 160
- *Adding a device* on page 161
- *Replacing a device* on page 162
- *Changing the IP address of a device* on page 163
- *Changing the cards or ports in a device* on page 163
- *Resetting the MTTR and MTBF* on page 164

The importance of unique IP addresses

Network Discovery relies mostly on device IP addresses for gathering statistics and information. It is important to have unique IP addresses for all your devices and their components.

If you have duplicate IP and MAC addresses in your network, you may have difficulty obtaining accurate device and port statistics.

If you do have duplicate IP or MAC addresses, you can purge the devices, then reassign the device addresses as necessary. Network Discovery will then rediscover the devices and map them properly.

This section features several possible scenarios, for adding, removing, or replacing devices and ports in your network. If you experience problems and cannot find help in the documentation, contact your Network Discovery Customer Support representative.

Note: When you remove a device from the network, purge the device. This will ensure that it is no longer in the database.

Note: When you replace a device, or when you change cards within a device, it is a good idea to reset the MTTR (Mean Time to Repair) and MTBF (Mean Time Between Failures).


Removing a device

Network Discovery automatically trashes and purges a device that has been removed from the network. However, if you want to remove the device from the Network Map yourself, follow this procedure.

To purge a device from the network—starting from the Network Map

- 1 Physically remove the device from your network following your company's standard procedures.
- 2 Locate the device on the Network Map using the **Find** tool.
- 3 With the device icon selected, **Object > Purge**.
A confirmation message appears.
- 4 Click **Purge**.

To purge a device from the network—starting from the Device Manager

- 1 Click the **Purge device** button. 
A confirmation message appears.
- 2 Click **Purge**.

Adding a device

These procedures will be helpful when you are adding any new device to your network.

Note: If one or more of the ports on the device you add is the end of a Permanent Virtual Circuit (PVC), make sure you add the correct Committed Information Rate (CIR) to the Port Manager. See the *Reference Manual*.

With a new IP address

Once you have added a device to your network, Network Discovery will discover it automatically. If you want the device to appear on your map quickly, follow this procedure.

To make a new device appear on the Network Map quickly

- 1 From the main Toolbar, click the **Find** button.
- 2 In the Find window, enter the IP address or domain name of the new device.
A warning appears, saying that Network Discovery does not have the device in its database. However, a link to the device appears.
- 3 Click the link to open a Device Manager session.
- 4 In the Device Manager, click **Update Model**.

Network Discovery begins network discovery on the device immediately.

With the same IP Address as a trashed device

If a device has been trashed, and you are using that IP address for a new device, it is best to purge the old device.

By purging the trashed device, you will delete all statistics associated with that device. If you do not purge the trashed device, you may see mixed port statistics in the Device Manager. However, the device statistics will not be mixed.

In the case where the two devices have the same MAC address, the trashed device will appear to become active again. This will be updated, so the new device will appear on the map with the correct IP address.

Replacing a device

There are many reasons for replacing one of your network devices. Perhaps a device has been damaged, or you could be upgrading part of your network. Whenever you are replacing a network device, be sure to use one of the following procedures.

Note: If one or more of the ports on this device is the end of a Permanent Virtual Circuit (PVC), make sure you add the correct Committed Information Rate (CIR) to the Port Manager. See the *Reference Manual*.

With an identical device

If you are replacing one device with another of the same model, and the same MAC address, Network Discovery will see no difference between the two devices. Network Discovery will register a break alarm when the first device is shut down, but will clear that alarm when the new device is powered on.

If the new device has a different MAC address, it is best to purge the old device. Network Discovery will eventually purge the old MAC address (according to your purge interval settings), and discover the new MAC address and map the new device.

With a different device

When you replace a device with a different device, it always best to purge the old device before adding the new device.

Changing the IP address of a device

There are several reasons why you may be changing the IP address for a device. Some common reasons are:

- You have been changing your subnets.
- You assigned an IP to a device, but discovered that the IP is not allowed because it falls within a reserved IP range.
- You have accidentally created a duplicate IP in your network, and need to change one of the addresses.

Changing the IP address of the device does not affect how Network Discovery sees the network. Read the following notes to make sure you understand how Network Discovery reacts.

Note: If you change the IP of the device, but the MAC remains the same, the Network Discovery database updates automatically.

Note: If you change the IP of a port, Network Discovery automatically discovers the change. No additional action is required.

Note: If you change the IP of the device, and the MAC is not known, the update is slightly delayed.

Changing the cards or ports in a device

If you change all the cards in a device (and they have all new MAC addresses), Network Discovery reads the device as a completely new device.

If you change all but one card in a device, the new information is temporarily merged with the old information. The new ports are discovered automatically, but the old ports remain in the database until they are aged out. This means there may be some duplicate ports listed in the Device Manager.

The best procedure is to purge the device before you change its ports or purge the old ports. Then, Network Discovery rediscovers the device as if it were new.

To purge a device from the network—starting from the Network Map

- 1 Physically remove the device from your network following your company's standard procedures.
- 2 Locate the device on the Network Map using the Find tool.
- 3 With the device icon selected, **Object > Purge**.
A confirmation message appears.
- 4 Click **Purge**.

To purge a device from the network—starting from the Device Manager

- 1 Click the **Purge** button.
A confirmation message appears.
- 2 Click **Purge**.

To purge a port from a device

- 1 In the Ports Manager, click the **Purge a port** button.
A confirmation message appears.
- 2 Click **Purge**.

Note: If one or more of the ports on this device is the end of a Permanent Virtual Circuit (PVC), make sure you add the correct Committed Information Rate (CIR) to the Port Manager. See the *Reference Manual*.

Resetting the MTTR and MTBF

An Administrator account can reset the MTBF (Meant Time Between Failures) value of a device. Resetting the MTBF is useful when you install new firmware in a device or when you replace devices that have been broken and then repaired.

Warning: Clicking **Reset MTTR and MTBF** with a package selected resets the values for each object within the package (that is, recursively).

- 1 On the Network Map, with an icon or multiple icons selected, **Object > Reset MTTR and MTBF**.

Note: You will also find **Reset MTTR and MTBF** on right-click menus for packages and multiple objects.

A confirmation message appears.

2 Click **Reset**.

14 | Deleting Data, Connections, and CHAPTER | Devices

This section is for Administrator accounts only.

Do not perform these procedures unless you completely understand the consequences.

After you delete connections, Network Discovery will start building connections again. This could take a long time, especially in large networks.

By changing the trash and purge intervals, you risk removing devices from your network that would not be removed with the default settings.

If you are unsure of the consequences of these actions, read the appropriate sections of the *Reference Manual* or contact Peregrine Systems Customer Support.

Topics in this chapter include:

- *Deleting data* on page 168
- *Deleting connections* on page 169
- *Changing the device trash and purge (expiry) intervals* on page 170
- *Changing the device purge intervals* on page 171

Deleting data

The following procedures delete data and statistics for your network stored on your appliance. Depending on the option chosen, they can also delete data used to configure the appliance.

Warning: Deleting network data and statistics stored on your appliance is an extremely drastic action that cannot be undone. Consider making a backup of your data first. See the *Network Discovery Setup Guide*.

There are three options, of increasing severity:

- *Network data:* the Network Discovery database of your network devices are deleted, along with device statistics, events, reports, and time warp databases
- *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. The only things left remaining will be:
 - the operating system
 - the Network Discovery software
 - the IPv4 address, netmask and gateway that you entered in the configuration interface

To delete Network Discovery data

- 1 Click **Administration > Data management > Delete data**.
- 2 Select one of the following:
 - Network data
 - Above plus accounts
 - Above plus configuration data and internal backup

3 Click Delete Data.

Figure 14-1: Deleting data

Network data (network map, events, statistics reports, scan files, and forecast views)
 Above plus accounts
 Above plus configuration data and internal backup

Send e-mail when data deletion done: Yes No

E-mail address:

Home > Administration > Data > Delete Data

Deleting connections

This procedure will delete connections between objects on the Network Map. It will take a few moments for changes to be reflected in the map.

You can choose to delete:

- all the connections that have been made, both those established by Network Discovery and those defined by the user
- just the connections defined by the user

If you delete all connections, Network Discovery will start over in its attempts to establish connections between objects. User-defined connections will not be re-established by Network Discovery, no matter which of the two options you select.

To delete all connections

- 1 Click **Administration > Data management > Delete connections**.
- 2 Click **All**.
- 3 Click **Delete Connections**.
- 4 Click **Confirm**.

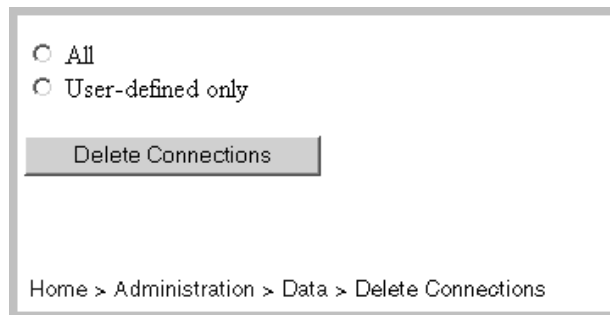
Both automatic and user-defined connections are deleted.

After connections are deleted, Network Discovery will restart its attempts to establish automatic connections between objects. It will not reconstruct user-defined connections.

To delete user-defined connections

- 1 Click **Administration > Data management > Delete connections**.
- 2 Click **User-defined only**.
- 3 Click **Delete Connections**.
- 4 Click **Confirm**.

Figure 14-2: Delete connections



Changing the device trash and purge (expiry) intervals

A trash interval refers to the length of time Network Discovery will wait before it moves a “not seen” device into the trash. The interval should be long enough that devices are allowed to be turned off for long periods, but short enough that devices removed from the network are not needlessly monitored.

Devices in the trash disappear from the Network Map and reports, but their statistical information is preserved in the event that the devices are returned to an active state before they are permanently purged.

There are three trash intervals, one each for devices with:

- SNMP management

- no SNMP management

Whether or not the trash interval is accepted depends on your Device Modeler Interval. See the *Reference Manual* for more details.

Figure 14-3: Device Trash Intervals and Purge Intervals

Device Trash Intervals

Managed devices trash interval: Weeks: Days: Hours:

Unmanaged devices trash interval: Weeks: Days: Hours:

Device Purge Intervals

Managed devices purge interval: Weeks: Days: Hours:

Unmanaged devices purge interval: Weeks: Days: Hours:

Home > Administration > Network Tuning > Expiry

To change the device trash intervals

- 1 Click **Administration > Network tuning > Expiry > Device Trash Intervals**.
- 2 Enter the values for the time for managed, unmanaged and scanned-only devices.
- 3 Click **Change**.

Changing the device purge intervals

The device purge interval starts when the device has been placed in the trash. The purge interval refers to the length of time Network Discovery waits before it purges a device that has been moved to the trash. The interval 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.

Devices that are purged disappear from the Network Map and their statistical information is destroyed. (Contrast this with the trash, in which statistical information is preserved.) Once a device has been purged, the ping and poll process will rediscover the device, if it has not been disconnected.

There are two purge intervals, one each for devices with:

- SNMP management
- no SNMP management

The interval for managed devices can be 1–12 weeks in length. The interval for unmanaged devices can be 1–12 weeks in length. The interval for managed devices should be greater than or equal to the interval for unmanaged devices. the default for both is 4 weeks.

To change the device purge intervals

- 1 Click **Administration > Network tuning > Expiry > Device Purge Intervals**.
- 2 Enter a values for the time for managed, unmanaged and scanned-only devices.
- 3 Click **Change**.

15

CHAPTER

Connecting with Another Management System

You can access other element management systems from Network Discovery. Also, you can access Network Discovery from the other element management systems.

Because all of Network Discovery's components are web-based, you can link to the URL of any part of Network Discovery accessible from the main Toolbar.

Topics in this chapter include:

- *Connecting from Network Discovery to another system on page 174*
- *Connecting to Network Discovery from another system on page 175*

Connecting from Network Discovery to another system

You can connect to as many as eight other element management systems from Network Discovery. Once you have entered a target URL, you can access the other system from any Device Manager window. You can launch an application or a URL. The element manager can be launched on a specific device, either from a map window or from the Device Manager.

Setting up the default URL or application

Network Discovery can automatically provide your element manager with the identity of the device—either its IP address or its MAC address. If your element manager identifies a device by its IPv4 address, you should include [IPv4] at the appropriate place in the URL. If a MAC address is required, include [MAC] in the URL. Network Discovery will automatically replace [IPv4] or [MAC] with the address of the active device.

Note: To force updating of Names in the map window, you must first click *Change*. If you had a map session or Health Panel open when you made the change, you should close and reopen the map or Health Panel.

To setup a connection to another Element Management System

- 1 Click **Administration > Display preferences > Element management**.
For each element manger to be added:
- 2 Enter the name of the other management system.
- 3 Enter the complete URL (beginning with http://).

4 Click Change.

Figure 15-1: Setting up the Default URL

Number	Name	URL or Executable
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>

Home > Administration > Display > Element Management

Opening the other system

Once you have the element management system URL entered into Network Discovery, you can access the other system in two ways:

- From the Device Manager, click the **Manage** button.
- From the Network Map, click **Object** > [Element Management].

In the **Object** menu, an item appears with the name you assigned in *Setting up the default URL or application* on page 174.

Connecting to Network Discovery from another system

Another element management system, Web pages, or other documents can launch major components of Network Discovery., including the Device Manager, Port Manager, Line Manager, and all features associated with the main Toolbar.

To launch a component from outside Network Discovery use “?go=” commands. The “?go=” commands associated with the main Toolbar require only a single argument. The “?go=” commands associated with the Managers can have multiple arguments.

To launch a component on a remote Network Discovery Appliance from an Appliance running in Aggregator mode, use the optional argument “remote_ip”.

Optional arguments are shown in [square brackets]. Variables (which you must replace with a value) are shown in angle brackets and *<this font>*. Omit the square brackets, angle brackets and spaces between arguments when you type the actual text.

Device Manager

Insert the following text to create a link to the Device Manager.

```
http://<my_appliance>/nm/?go=device ;device=<device_id>
[;device_type=<device_type>] [;panel=<panel>]
```

Table 15-1: Text for the Device Manager

Parameter	Description
device_id	any string
device_type	one of: OID, NMID, PortOID, PortNMID, IP, IPv4, IPv6, MAC, Cloud, DNS, Label, LabelPrefix, NetBIOS
panel	one of: about, state, stats, ports, events, ip_ping, traceroute, snmp_ping, dns, jaywalk (if omitted, uses account's default)

Examples

- `http://nmappliance.example.com/nm/?go=device;device=172.17.1.1`
(opens device by IP address)
- `http://nmappliance.example.com/nm/?go=device;device=172.17.1.1;device_type=IPv4` (opens device by IP address; more efficient)
- `http://nmappliance.example.com/nm/?go=device;device=56;device_type=NMID` (opens device by the Peregrine appliance internal ID)

Port Manager

Insert the following text to create a link to the Port Manager.

```
http://<my_appliance>/nm/?go=port [&device=<device_id>
[&device_type=<device_type>] &port=<port_id> [&port_type=<port_type>]
[&panel=<panel>]
```

Table 15-2: Text for the Port Manager

Parameter	Description
device_id	any string
device_type	one of: OID, NMID, PortOID, PortNMID, IP, IPv4, IPv6, MAC, Cloud, DNS, Label, LabelPrefix, NetBIOS
port_id	any string
port_type	one of: OID, NMID, Index, Description
panel	one of: about, diagnosis, stats, events (if omitted, uses account's default)

Examples

- `http://nmappliance.example.com/nm/?go=port;device=172.17.1.1;port=eth0` (opens port by IP address and description)
- `http://nmappliance.example.com/nm/?go=port;port=238;port_type=NMID` (opens port by the Peregrine appliance internal ID)

Line Manager

Insert the following text to create a link to the Line Manager.

```
http://<my_appliance>/nm/?go=line [&device=<device_id>]
[&device_type=<device_type>] &port=<port_id> [&port_type=<port_type>]
[&panel=<panel>]
```

Table 15-3: Text for the Line Manager

Parameter	Description
device_id	any string
device_type	one of: OID, NMID, PortOID, PortNMID, IP, IPv4, IPv6, MAC, DNS, Label, LabelPrefix, NetBIOS
port_id	any string
port_type	one of: OID, NMID, Index, Description
panel	one of: about (if omitted, uses account's default)

This works the same as the Port Manager. The only additional restriction is that the Line Manager will only work if the specified port is connected to something. You may specify either end of the line.

Examples:

- `http://nmappliance.example.com/nm/?go=line;device=172.17.1.1;port=eth0` (opens line by IP address and description)
- `http://nmappliance.example.com/nm/?go=line;port=238;port_type=NMID` (opens line by the Peregrine appliance internal ID)

Attribute Manager

Insert the following text to create a link to the Attribute Manager.

```
http://<my_appliance>/nm/?go=attribute [&device=<device_id>]
[&device_type=<device_type>] [&port=<port_id>] [&port_type=<port_type>]
[&attribute=<attribute_id> [&attribute_type_type=<attribute_type>]
[&panel=<panel>]
```

Table 15-4: Text for the Attribute Manager

Parameter	Description
device_id	any string
device_type	one of: OID, NMID, PortOID, PortNMID, IP, IPv4, IPv6, MAC, Cloud, DNS, Label, LabelPrefix, NetBIOS
port_id	any string
port_type	one of: OID, NMID, Index, Description
panel	one of: about, stats (if omitted, uses account's default)
attribute_id	any string
attribute_type	one of the following: NMID, Name (valid attribute_id when attribute_type=Name are the following:)

Attribute name	Description
in_util	Average Line In Utilization
out_util	Average Line Out Utilization
full_util	Line Utilization
delay	Delay
jitter	Jitter
in_bytes	Bytes In
out_bytes	Bytes Out
in_frames	Frames In
out_frames	Frames Out
in_unicasts	Unicasts In
out_unicasts	Unicasts Out

Attribute name	Description
in_broadcasts	Broadcasts In
out_broadcasts	Broadcasts Out
collisions	Collisions
in_errors	Errors In
out_errors	Errors Out
cir_headroom	CIR (Committed Information Rate) Headroom
cir_shortfall	CIR Shortfall
data_delivery_ratio	Data Delivery Ratio
frame_delivery_ratio	Frame Delivery Ratio
in_frde	Discard Eligibility In
out_frde	Discard Eligibility Out
bcn	
fecn	
breaks	Breaks
downtime	Downtime
drops	Packet Loss
total_in_util	Total In Utilization
total_in_bytes	Total In Bytes
total_in_frames	Total In Frames
total_in_unicasts	total In Unicasts
total_out_unicasts	Total Out Unicasts
total_in_broadcasts	Total In Broadcasts
total_collisions	Total Collisions
total_errors	Total Errors
cpu	CPU
load	Load Average
ram	Memory
vram	Virtual Memory

Attribute name	Description
disk	Disk
bp_util	Backplane Utilization
status	Operational Status
port_on_off	
bridge_aging	Bridge Aging Interval
printer_status	Printer Status
toner	Toner
paper_count	Paper Count
paper_status	Paper Status
total_paper	Pages printed
changes	Changes
news	Network Early Warning System
mttr	mean Time to Repair
mtbf	Mean Time Between Failures

Examples:

- http://nmappliance.example.com/nm/?go=attribute;device=172.17.1.1;port=eth0;attribute=in_util;attribute_type=Name (opens attribute by IP address and description and show the utilization in attribute)
- http://nmappliance.example.com/nm/?go=attribute;attribute=49234;attribute_type=NMID (opens attribute by the Peregrine appliance internal ID)

Service Analyzer

Insert the following text to create a link to the Service Analyzer.

```
http://<my_appliance>/nm/?go=service_analyzer ;device1=<device_id>
[;device1_type=<device_type>] ;device2=<device_id>
[;device2_type=<device_type>]
```

Table 15-5: Text for the Service Analyzer

Parameter	Description
device1_id	any string
device1_type	one of: OID, NMID, PortOID, PortNMID, IP, IPv4, IPv6, MAC, Cloud, DNS, Label, LabelPrefix, NetBIOS
device2_id	any string
device2_type	one of: OID, NMID, PortOID, PortNMID, IP, IPv4, IPv6, MAC, Cloud, DNS, Label, LabelPrefix, NetBIOS

Examples:

- `http://nmappliance.example.com/nm/?go=service_analyzer;device1=172.17.1.1;device2=nmc`
- `http://nmappliance.example.com/nm/?go=service_analyzer;device1=32;device1_type=NMID;device2=78;device2_type=NMID` Other components

Other components

As stated above, you can create a link to any part of Network Discovery that is accessible from the main Toolbar.

Table 15-6: Text to link to all the other major features of Network Discovery.

Module	Command
Health Panel	<code>http://<my_appliance>/nm/?go=health_panel</code>
Network Map	<code>http://<my_appliance>/nm/?go=network_map</code>
Events Browser	<code>http://<my_appliance>/nm/?go=events</code>

Module	Command
Service Analyzer Query	<a href="http://<my_appliance>/nm/?go=service_analyzer_query">http://<my_appliance>/nm/?go=service_analyzer_query
Find	<a href="http://<my_appliance>/nm/?go=find">http://<my_appliance>/nm/?go=find
MIB Browser	<a href="http://<my_appliance>/nm/?go=mib_browser">http://<my_appliance>/nm/?go=mib_browser
Home	<a href="http://<my_appliance>/nm/?go=home">http://<my_appliance>/nm/?go=home
Status	<a href="http://<my_appliance>/nm/?go=status">http://<my_appliance>/nm/?go=status
Reports	<a href="http://<my_appliance>/nm/?go=reports">http://<my_appliance>/nm/?go=reports
Administration	<a href="http://<my_appliance>/nm/?go=administration">http://<my_appliance>/nm/?go=administration
Help	<a href="http://<my_appliance>/nm/?go=help">http://<my_appliance>/nm/?go=help

16

Vacations and Weekends

CHAPTER

This section is for the Network Discovery Administrator only.

When you are going to be away from work for a long period of time, there are a few things you can do to make sure you find out about what happened while you were gone.

Even though you will likely assign your network responsibilities to someone else, you may still need to know what happened while you were away.

Topics in this chapter include:

- *Before you go away* on page 186
- *When you come back* on page 187

Before you go away

By setting up a few things before you go away, you can make your job much easier when you get back.

Set the Trash and Purge intervals

Before a plant shutdown (for example, at Christmas), you may want to increase the Trash/Purge intervals, if you have set them to be fairly short. Otherwise, Network Discovery won't see all the workstations that are shut down for the holidays and may remove them from its model of the network.

To change Trash and Purge Intervals

Administration > Network tuning > Expiry > Device Trash Intervals

On the other hand, if you are just going away on your own vacation, you will probably leave the trash and purge intervals the same and just let your substitute monitor the network.

For more information, see *Changing the device trash and purge (expiry) intervals* on page 170

Change who will be notified when events occur

Don't forget to change the address of the person who will be paged or e-mailed when you are unavailable.

To change the e-mail address to which Network Discovery sends notification of problems

- 1 Click **Administration > Appliance administrator e-mail address**
- 2 Replace your e-mail address with the your substitute's e-mail address.
- 3 Click **Change**.

Note: You must already have set up your substitute's account. You may have to give your substitute Administrator account privileges. For instructions on setting up accounts, see *Setting up Accounts* on page 23

When you come back

You can monitor events in a few different ways, depending on what you want to see:

- Check the Network Map and Health Panel to see current network faults.
- Use the Events Browser to view alarms and warnings specific to particular times.
- View Fault Summary reports to view alarms and warnings over longer periods of time.

When you come back after a weekend, check to see if anybody added, removed, or modified any devices in your network.

Look for changes on the Network Map

- 1 On Monday morning, open the Network Map open and click **Edit > Alarm Thresholds**.
- 2 In the **General** tab, set the time to measure **Changes** to 64 hours in the **Alarm** field.
- 3 Click **Apply**.

Network Discovery may find that the network has several problems that were not present 64 hours ago on Friday afternoon. On the Network Map any device (of appropriate priority) that has been moved, added, or removed from the map since Friday will be highlighted with an alarm ring.

Top priority

Check for any current emergencies that need your attention right now.

- Check the Main Map and Health Panel for serious alarms to major devices.
- For any problematic device, check the Device Manager and Statistics for that device.
- Use the Service Analyzer tool to check paths for devices about which the users are concerned.
- Check Reports for major issues from the last few days.

Second priority

Once you have dealt with the emergencies, you will want to check on the other problems that happened while you were away, specifically on priority 3, 4, 5, and 6 devices. These may be intermittent problems that can cause network delays or outages in the future.

Some good questions for your substitute administrator would be:

- How long did it take to fix them?
- What was the cause of the problem?
- Who fixed them and how?

Other ways to check for the problems would be to check:

- the Events Browser for alarms before a certain date
- Performance Summary and Fault Summary reports for all types of alarms and warnings
- other reports depending on the contents of your network

Third priority

You will likely want to check what Changes (adds and deletes) have occurred in your network while you were gone. This will allow you to see how the contents of your network have changed (if anyone has added or removed network equipment without informing you).

You will want to check the Network Map and Health Panel. Click the Changes button on the Health Panel to see what devices have alarms or warnings. Check the Changes Health Panel report to see:

- what devices have been added recently
- what devices have been moved recently
- what devices have not been seen recently

Checking individual devices

If you are concerned about any devices in particular, you should check the Device Manager and Port Manager windows for those devices. Concentrate on the Statistics panel, but you would also want to check the information on the State and Events panels.

17

Using an Aggregator

CHAPTER

If you have received an Aggregator license, this chapter will show you how to set up and use the Network Discovery Aggregator. To use the Aggregator, all of your Peregrine appliances must be at least InfraTools Network Discovery version 4.2.0.

Topics in this chapter include:

- *What's an Aggregator?* on page 190
- *How do I use the Aggregator?* on page 190
- *Installing your Aggregator license* on page 191
- *Setting up the Aggregator and remote appliances to work together* on page 192
- *Using the Aggregate Health Panel* on page 199
- *The Aggregate Events Browser* on page 201
- *Navigating through multiple appliances* on page 195

What's an Aggregator?

The Aggregator is a Peregrine appliance with a license that also allows it to collect and combine data from several Peregrine appliances in your network. The health data is combined into one Aggregate Health Panel, so you can see the status of the entire network. An Aggregator also allows you to access other individual Peregrine appliances without logging into them directly.

You can aggregate up to 10 Peregrine appliances with a maximum of 50,000 devices. However, the more appliances you aggregate, the more slowly the Aggregator processes the data. While performing as an Aggregator, the Peregrine appliance can also serve as a regular appliance, monitoring up to 100 devices.

It is important to remember what is aggregated, and what is not. The following functions are aggregated:

- Health Panel
- Events Browser

The following functions are not aggregated in any way:

- Network Map
- Find
- Events notification by e-mail, pager or SNMP trap

However, you *can* access these functions on remote appliances by means of the Aggregator.

How do I use the Aggregator?

An Aggregator Peregrine appliance works like a regular Peregrine appliance. The Aggregator has an extra license that allows it to collect data from the other Peregrine appliances in your network. The Aggregator can also be responsible for monitoring a specific part of the network, while simultaneously collecting data from other Peregrine appliances and presenting them in the Aggregate Health Panel.

There are many ways you could set up aggregation in your network, depending on the network topology and how many Peregrine appliances you have installed.

- You can use the Aggregator as a regular appliance to monitor a part of your network, as you would with any of your Peregrine appliances.
- You can use the Aggregator as a regular appliance to monitor only the backbone of your network, your important routers and servers, as well as the other Peregrine appliances.

If you have the resources available, we recommend option 2. You can use the other appliances to monitor the subnets, but this will give you a real center point from which you can access the rest of your network.

Installing your Aggregator license

Only one Peregrine appliance on your network needs to have the Aggregator license. So, you must decide which appliance that will be. If you are not sure how to decide, contact Peregrine Systems Customer Support.

You can request a license from Peregrine Systems Customer Support through the Network Discovery interface. For information on how to request and install a license, see *Licenses* in the *Network Discovery Setup Guide*. (If your aggregate license was installed on the appliance before you received it, you can skip this procedure.)

The Aggregate Toolbar

The Aggregate Toolbar has one extra row of buttons above the buttons included in the regular Toolbar.





Figure 17-1: Aggregate Toolbar

Extra row of buttons shows that this Toolbar belongs to an Aggregator



The extra Aggregate-specific buttons are listed in the following table. Note the “globe” symbol in each icon.

Table 17-1: Extra row of Aggregator buttons and their functions

Icon	Button name	Description
	Aggregate Health Panel	Opens the Aggregate Health Panel.
	Aggregate Events Browser	Opens the Aggregate Events Browser.
	Remote Appliances	Opens a page showing all the remote appliances that are configured to work with the Aggregator.
	Appliance pull-down list	Changes the context of the Toolbar buttons.

The buttons in the bottom row are the same as the buttons on a single appliance Toolbar. They affect only the Peregrine appliance you have selected from the Appliance pull-down list.

Setting up the Aggregator and remote appliances to work together

For the Aggregator to work, you must prepare the Aggregator and you must prepare each individual appliance. You give the Aggregator:

- the IP address of the remote appliance
- the remote account
- the Aggregate health update interval
- the Aggregate events update interval
- proxy use

On each individual Peregrine appliance you set up an account that allows access to the Aggregator.

To set up the Aggregator to access a remote appliance

- 1 On the Aggregator, click **Administration > Remote appliance administration > Add a remote appliance**.

- 2 Enter the IP address and the name of the remote appliance.
- 3 Click **Add**.
- 4 Click **Modify Properties**.
- 5 Enter a remote account (example, “admin”) to collect data for the Aggregate Health Panel.
- 6 Select an Aggregate health update interval.
Note: Here are some things to consider. More frequent updates use more more bandwidth.
- 7 Select an Aggregate events update interval.
Note: If you are using proxy services, be sure to read *Using Proxy Services* on page 203. If you are not using proxy services, skip step 8 and go to step 9.
- 8 If you are using proxy services, select one of the proxy options.
 - no proxy
 - proxy via local appliance
 - proxy via local appliance and remote appliances
 - proxy via remote appliance
- 9 Click **Change**.

Setting up the remote appliances for access

In order for the Aggregator to access Peregrine appliances in your network, you must have identical accounts on each Peregrine appliance that you want to aggregate.

Important: Repeat this procedure on each Peregrine appliance.

For example, if you have an Administrator account “kevin” on the Aggregator, you must have an Administrator account “kevin” on each remote appliance. The two accounts must have the same password. If the Aggregator and the remote appliances do not have identical accounts:

- the Aggregator and the remote appliances will not be able to communicate with each other
- you will not be able to access the remote appliances through the Aggregator

This procedure explains the minimum setup required to access the remote appliances. For more information on account setup, see *Setting up Accounts* on page 23.

To add an account

- 1 On the remote appliance click **Administration > Account administration > Add an account**.
- 2 Enter a login name.

The account name must be 3–20 characters long. Acceptable characters are:

- a through z
- 0 through 9
- underscore (_) (the underscore cannot be the first character in the account name)

Note: Uppercase letters are not acceptable.

- 3 Click **Add Account**.

A new screen appears, where you can modify account properties, contact data, and the password.

- 4 Click **Modify account properties**.
- 5 Select an account type from the list box.

Note: You cannot change the account type for the account you are currently using.

- 6 Enable the account for Web Access by selecting “Yes”.

Note: You cannot change the Web Access for the account you are currently using.

Note: If no password is given, the account cannot be used to log in, even when login status is set to “yes”.

7 (optional) Enter a descriptive name in the Name field.

8 Click **Modify Properties**.

A new screen appears, where you can modify account contact and the password.

9 Click **Modify account password**.

10 Enter the new password in the first field.

Do not enter the current password (if any).

Passwords can be up to 20 characters long. Acceptable characters are:

- A through Z
- a through z
- 0 through 9
- underscore (_)
- at (@)
- period (.)
- hyphen (-)

11 Enter the same new password in the second field.

Entering the same password twice helps guard against typing errors.

12 Click **Modify Password**.

You have finished setting up the account on one remote appliance. Now, you must repeat this procedure for each remote appliance the Aggregator needs to access.

Note: When you access a remote appliance by means of the Aggregator, the user preferences set on the Aggregator override those on the remote appliance.

Navigating through multiple appliances

There are two ways to switch appliance views:

- using the appliance pull-down list on the main Toolbar
- using the Remote Appliances list from the HomeBase page

Note: You must be careful, because this flexibility allows you to open windows for any number of remote appliances at the same time. The window you are looking at may be showing you:

- aggregated data
- unaggregated data from the Aggregator itself
- data from any of your remote appliances.

To be sure what you are looking at, check the name in the banner at the top of the window.

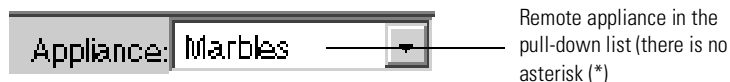
Using the pull-down list on the Toolbar

When you select a remote appliance from the pull-down list, you can use the Toolbar buttons to navigate the remote appliance.

For example, let's say your Aggregator is called "ExampleCorps." You want to open the Administration page for the remote appliance "Marbles." Select Marbles from the Toolbar pull-down list, then click the Administration button, and you will see the Marbles Administration page.

Note: Your local Aggregator always appears at the top of the list with an asterisk (*).

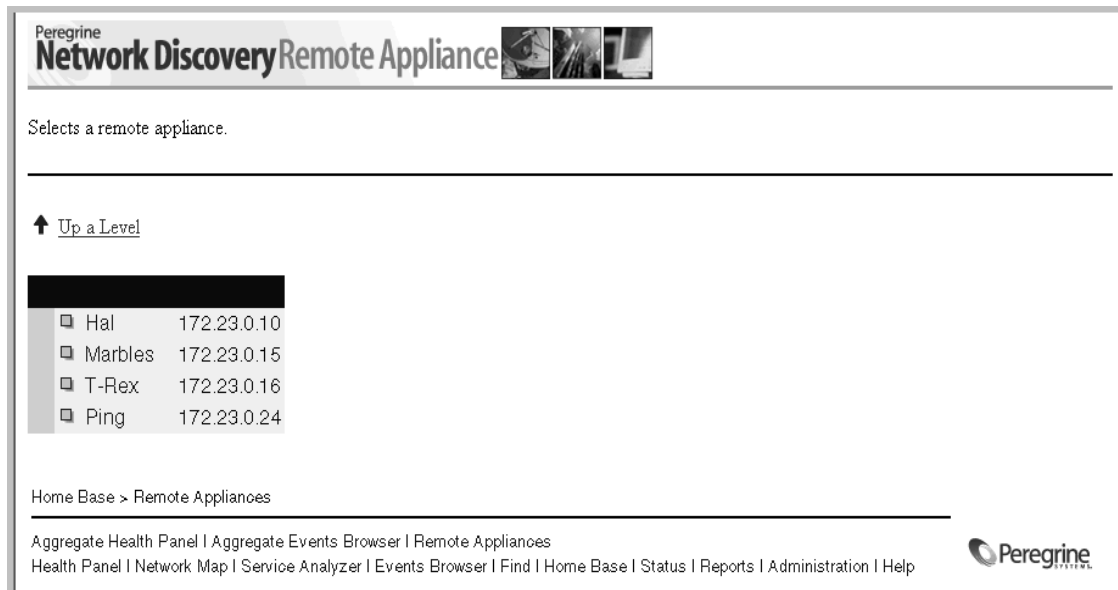
Figure 17-2: Remote appliance pull-down list



Using the Remote Appliances list

When you select a remote appliance from the Remote Appliances list, you can use the hyperlinks at the bottom of the HTML pages to navigate through the remote appliance. The Toolbar buttons only work with the remote appliance selected from the pull-down list.

Figure 17-3: Remote Appliances list



Peregrine
Network Discovery Remote Appliance


Selects a remote appliance.

[↑ Up a Level](#)

<input type="checkbox"/>	Hal	172.23.0.10
<input type="checkbox"/>	Marbles	172.23.0.15
<input type="checkbox"/>	T-Rex	172.23.0.16
<input type="checkbox"/>	Ping	172.23.0.24

Home Base > Remote Appliances

Aggregate Health Panel | Aggregate Events Browser | Remote Appliances
Health Panel | Network Map | Service Analyzer | Events Browser | Find | Home Base | Status | Reports | Administration | Help

 Peregrine

The difference between Home and Home Base

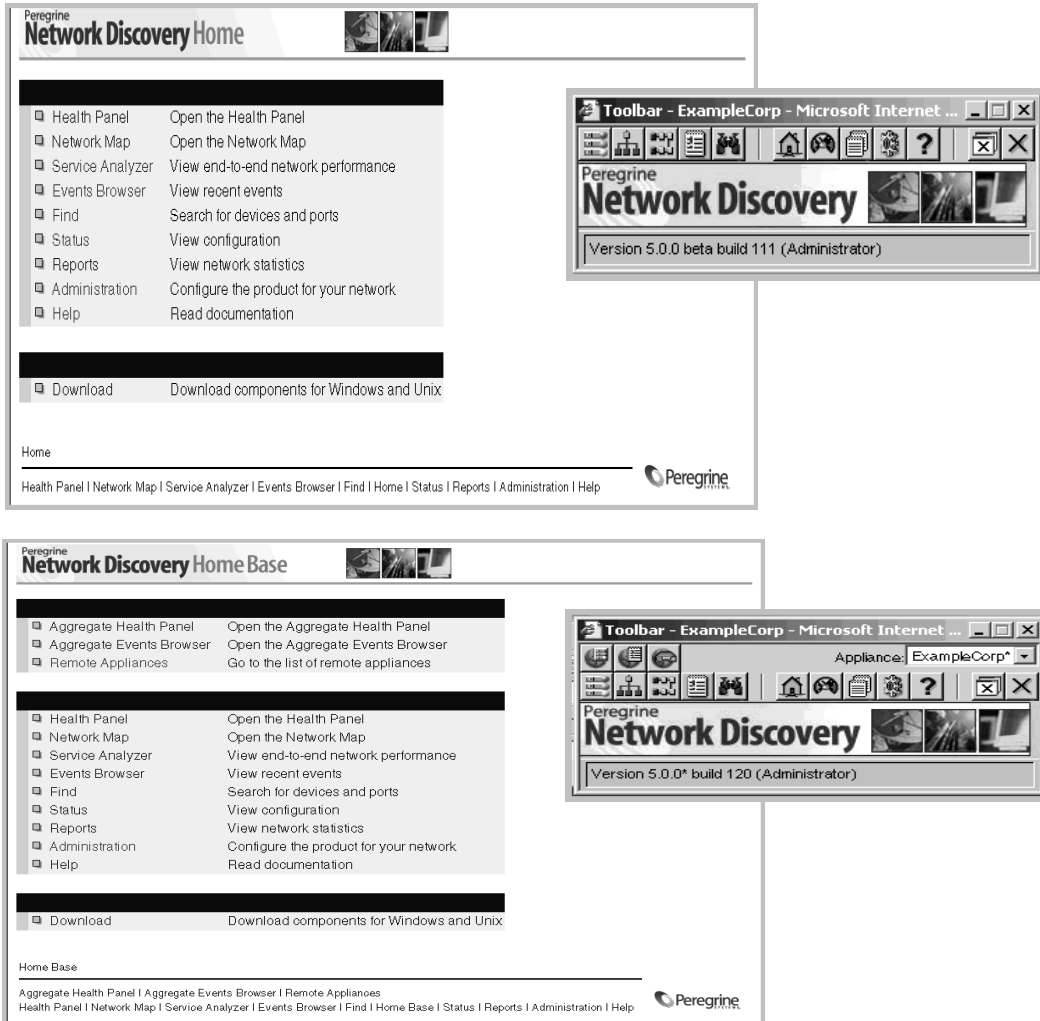
When you log into a regular Peregrine appliance, you see the Toolbar and the Home page.

When you log into an Aggregator Peregrine appliance, you see the expanded Toolbar and the Home Base page.

When you access a remote appliance from the Aggregator, you see that remote appliance's Home page.

Tip: To be sure you're looking at the right data, check the banner at the top of the page.

Figure 17-4: Home and Home Base



Using the Aggregate Health Panel

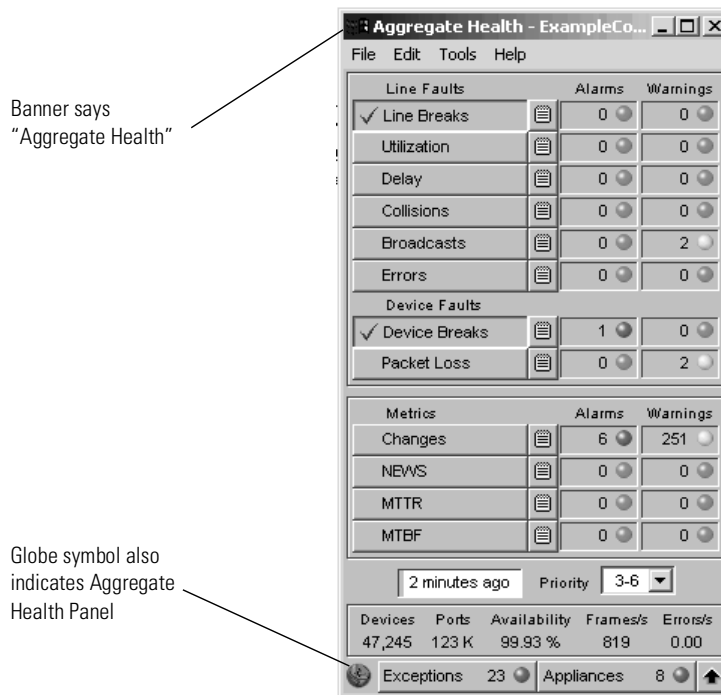
The Aggregate Health Panel looks similar to the regular Health Panel; it has all the same buttons and statistics. However, the Aggregate Health Panel combines all the statistics from all the aggregated Peregrine appliances in your network.

You can click on the report buttons to see complete lists of all events in the entire network. If you were looking at a regular Health Panel for one appliance, you would only see faults for a portion of your network.

Note: You can tell what Health Panel you're looking at by the report banner. If it is the Aggregator Health Panel, the banner says "Aggregate" rather than "Health Panel". A "globe" symbol in the lower left hand corner of the Health Panel also shows that you are looking at an Aggregator.

The statistics listed in the Aggregate Health Panel are the same as those listed in the regular Health Panel. For an explanation of what the statistics measure, see *See an overview with the Health Panel* on page 48.

Figure 17-5: The Aggregate Health Panel



Note: The Aggregator does not have a Network Map for aggregated data. A Network Map is always associated with an individual Peregrine appliance.

Note: If a device is included in the address scope of more than one Peregrine appliance, the device will appear more than once in the aggregated Health Panel reports. Each occurrence of the device will have a suffix, “[via <remote appliance name>]” to show you which appliance is reporting it.

Appliances button

Clicking the **Appliances** button at the bottom of the Health Panel takes you to the **Aggregate Appliance Health** page. This page shows you a summary of the health status of all your remote Peregrine appliances.

By clicking on any of the appliance hyperlinks on this page, you can see the **Appliance Health** page for that Peregrine appliance.

Note: The local Peregrine appliance is always at the top of the list with an asterisk (*).

Exceptions button

Clicking the **Exceptions** button at the bottom of the Health Panel takes you to the **Aggregate Appliance Exceptions** page. This page shows you a summary of all the exceptions appearing on the remote Peregrine appliances. Exceptions are elements in your network that are improperly configured (for example, an incorrect netmask). Exceptions prevent discovery and mapping of your network.

By clicking on any of the appliance hyperlinks on this page, you can see the **Exceptions Summary** page for that Peregrine appliance.

Note: The local Peregrine appliance is always at the top of the list with an asterisk (*).

For more information on exceptions, see the *Reference Manual*.

The Aggregate Events Browser

The aggregate Events Browser is almost identical to the regular Events Browser. However, events from an aggregated remote appliance have “[via Appliance name]” in the device/port column; events reported by the local appliance do not.

The Aggregator updates events hourly (by default). Due to the time lag, events may not be completely up to date.

If aggregation is turned on, but no Aggregators have been set up, the aggregate events browser will look very much like the regular events browser except for the time delay.

18 Using Proxy Services

CHAPTER

This chapter provides a cursory overview of the proxy services available with Network Discovery. You should have a high level of networking expertise to use this feature. If you are uncertain about how to set up this feature, you may want to contact Peregrine Systems Customer Support for help.

Warning: If you are unsure about how to use Proxy services, do not attempt to use this feature.

- Topics in this chapter include:
 - *Four examples* on page 204
 - *Using the default—no proxy* on page 204
 - *Proxy access through a remote appliance* on page 206
 - *Proxy access through the Aggregator* on page 207
 - *Proxy access through the Aggregator and remote appliances* on page 209

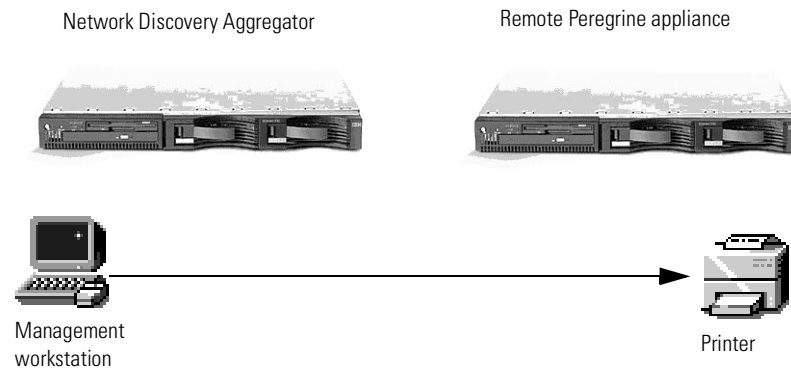
Four examples

We will cover four simple scenarios as examples. In each example, there are two Peregrine appliances (one Aggregator and one remote), a user's workstation, and a printer to which the user wants to open a telnet or HTTP session.

Note: When describing the relationship between the Aggregator and other Peregrine appliances, the documentation refers to the Aggregator as the “local” appliance, and the others as “remote” appliances.

Using the default—no proxy

Figure 18-1: Possibility one—direct HTTP/Telnet access



Description

This is the default scenario. Proxy services are not needed, because your users have direct HTTP/telnet access to the other devices in your network.

When you click the Web or Telnet buttons on the Device Manager, you directly access the device from your workstation. The connection does not go through the Peregrine appliance.

How to set it up

Since this is the default, you don't have to change anything. No configuration changes are needed. However, you *can* use this procedure to turn off the proxy services if you ever need to.

To set up on the remote appliances

Important: You must repeat this procedure on each remote Peregrine appliance in your network. If you do not set up all the remote Peregrine appliances, your proxy services will not work properly.

- 1 Log into the remote Peregrine appliance.
- 2 Click **Administration > Appliance services > Appliance proxy services**.
- 3 Select “Disable proxy services” (this is the default setting).
- 4 Click **Change**.

To set up on the Aggregator

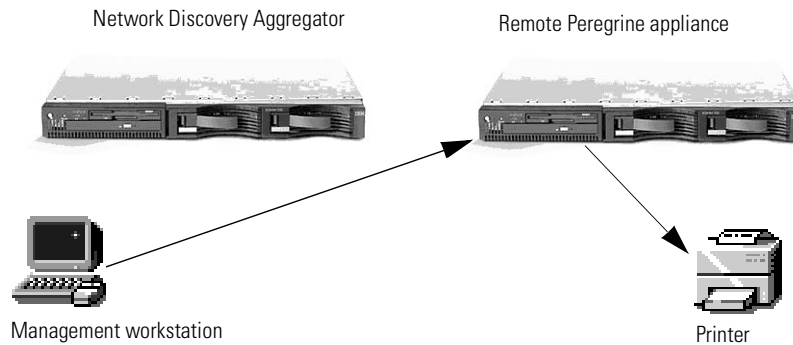
- 1 Log into the Aggregator Peregrine appliance.
- 2 Click **Administration > Appliance services > Appliance proxy services**.
- 3 Select “Disable proxy services” (this is the default setting).
- 4 Click **Change**.

You have turned off the Aggregator's proxy services. Now, you must tell the Aggregator how to proxy to each remote Peregrine appliance.

- 5 Click **Administration > Remote appliance administration > Remote appliance properties**.
- 6 Select a remote appliance from the pull-down list.
- 7 Click **Modify Properties**.
- 8 Select “no proxy” (this is the default setting).
- 9 Click **Change**.

Proxy access through a remote appliance

Figure 18-2: Possibility two—through a remote Peregrine appliance



Description

This scenario is best for users who might be accessing different networks. For example, a management service provider (MSP) may need to access data inside the network of their customer, another company.

Assuming the MSP has access through the customer firewall, the MSP can log in to the remote Peregrine appliance and from there, access data from the devices in the customer network.

How to set it up

To set up on the remote appliance

Important: You must repeat this procedure on each remote Peregrine appliance in your network. If you do not set up all the remote Peregrine appliances, your proxy services will not work properly.

- 1 Log into the remote Peregrine appliance.
- 2 Click **Administration > Appliance services > Appliance proxy services**.
- 3 Select “Enable proxy services.”

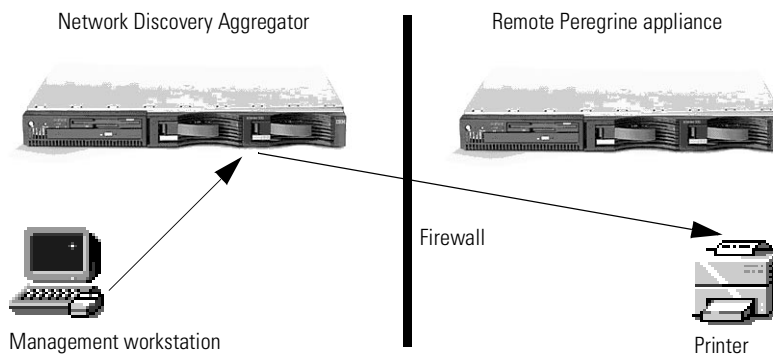
4 Click Change.

To set up on the Aggregator

- 1 Log into the Aggregator Peregrine appliance.
- 2 Click **Administration > Remote appliance administration > Remote appliance properties**.
- 3 Select a remote appliance from the pull-down list.
- 4 Click **Modify Properties**.
- 5 Click **proxy via remote appliance**.
- 6 Click **Change**.

Proxy access through the Aggregator

Figure 18-3: Possibility three—through the Aggregator



Description

Proxy through the Aggregator actually allows you to access the remote Peregrine appliance, which will access the device you want to see. In this case, a firewall is blocking your workstation's view of the remote Peregrine appliance, so you access the Aggregator first, and connect to the end device through the remote Peregrine appliances.

How to set it up

To set up on the remote appliance

Important: You must repeat this procedure on each remote Peregrine appliance in your network. If you do not set up all the remote Peregrine appliances, your proxy services will not work properly.

- 1 Log into the remote Peregrine appliance.
- 2 Click **Administration > Appliance services > Appliance proxy services**.
- 3 Select “Enable proxy services.”
- 4 Click **Change**.

To set up on the Aggregator

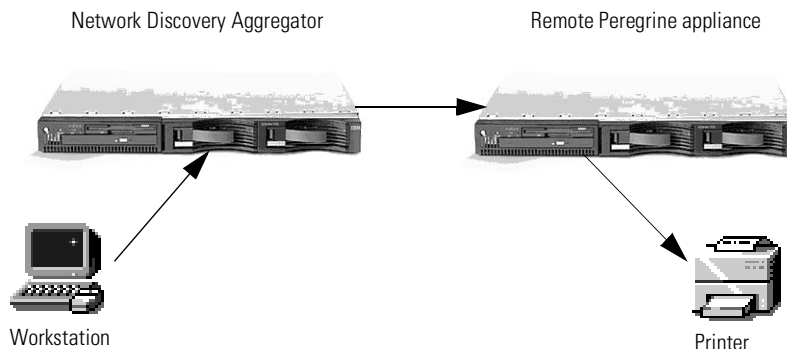
- 1 Log into the Aggregator Peregrine appliance.
- 2 Click **Administration > Appliance services > Appliance proxy services**.
- 3 Select “Enable proxy services.”
- 4 Click **Change**.

You have turned on the Aggregator’s proxy services. Now, you must tell the Aggregator how to proxy to each remote Peregrine appliance.

- 5 Click **Administration > Remote appliance administration > Remote appliance properties**.
- 6 Select a remote appliance from the pull-down list.
- 7 Click **Modify Properties**.
- 8 Click **proxy via local appliance**.
- 9 Click **Change**.

Proxy access through the Aggregator and remote appliances

Figure 18-4: Possibility four—through the Aggregator and remote Peregrine appliances



Description

In this scenario, a network could contain duplicate subnets. This might occur because you are an internet service provider (ISP), or maybe your company has recently acquired another company who used some of the same subnet IP addresses.

Each Peregrine appliance will monitor a particular subnet, and the Aggregator will combine the statistics from all the remote appliances.

You must turn on the proxy services for the Aggregator, so it will be able to connect with the remote Peregrine appliance, which will in turn connect with the devices in its subnet.

Note: The Aggregator is connecting to the remote appliance on the one port available for proxy services. This means that only one user can open a Web session at a time in this scenario. If the Web session is unused for five minutes, it times out and another user can access a Web session.

How to set it up

To set up the remote appliance

Important: You must repeat this procedure on each remote Peregrine appliance in your network. If you do not set up all the remote Peregrine appliances, your proxy services will not work properly.

- 1 Log into the remote Peregrine appliance.
- 2 Click **Administration > Appliance services > Appliance proxy services**.
- 3 Select “Enable proxy services.”
- 4 Click **Change**.

To set up on the Aggregator

- 1 Log into the Aggregator Peregrine appliance.
- 2 Click **Administration > Appliance services > Appliance proxy services**.
- 3 Select “Enable proxy services.”
- 4 Click **Change**.
You have turned on the Aggregator’s proxy services. Now, you must tell the Aggregator how to proxy to each remote Peregrine appliance.
- 5 Click **Administration > Remote appliance administration > Remote appliance properties**.
- 6 Select a remote appliance from the pull-down list.
- 7 Click **Modify Properties**.
- 8 Click **proxy via local appliance and remote appliance** (only select this one if you have already set up the Aggregator to use proxy services).
- 9 Click **Change**.

Index

Symbols

?go= commands 175

A

account

- adding an account 24
- aggregator setup 193
- changing name 26
- changing the type 26
- customizing a profile 26
- deleting 32
- listing user accounts 24
- modifying contact information 30
- modifying password 31
- modifying properties 36
- setting type 26
- types 17

- admin 20
- regular 19

Account capabilities

- MySQL ODBC Access 26
- Shared directory Access 26
- Web Access 26

account properties

- account type 26
- allow to copy map configurations 26, 36
- append IP address 26, 36
- default device panel 27, 37
- default port panel 27, 37
- help format 27, 37
- long date format 27, 36

- make URLs visible 26, 36

- name 26, 36

- short date format 27, 37

- status reports 26

admin account

- customizing the Network Map 91
- description 20

Administration

- account contact information 30

- account password, modifying 31

- account properties 36

- adding an account 24

- configuration files

- change default 114

- copy 113

- delete 113

- rename 114

- contact data 39

- customizing a user profile 26

- deleting an account 32

- deleting connections 169

- device trash intervals 170

- event filters 129

- delete 142

- list 142

- modify 140

- reset to defaults 143

- listing user accounts 24

- modify password 40

- Pager Service Provider Configuration 117

- purge controls 170

- restarting the appliance 16
- restore prime map configuration 115
- shutdown the appliance 15
- test e-mail address 41
- test pager address 42
- test pager number 42
- Aggregate Health Panel 199
 - appliances 200
 - exceptions 201
- Aggregator 189
 - home base 197
 - installing licence 191
 - navigating multiple appliances 195
 - remote appliances 192, 196
 - setting up 192
 - setting up accounts 193
 - toolbar 191
 - pull-down list 196
- alarm thresholds
 - changing 96
 - device types 96
 - general 98
 - line alarm types 97
- alarms
 - colors 88
- Analyze button, Service Analyzer 73
- appliance
 - navigation with aggregator 195
 - restart 16
 - shutdown 15
- Appliance Health 49
- Approximate 57
- Assistant window 27, 37
- Automatic packaging 103
 - preferences 107
- autosave 111

B

- background
 - grey 60
- blue line under icon 61, 106
- buttons
 - Analyze 73

C

- Carrier Network 57
- Changes
 - Health Panel report 188
 - setting thresholds 98
- checklist, when going away 185
- cloud icon 57
- clouds 57
 - carrier network icon 57
 - cloud icon 57
 - radio cloud icon 57
 - unmanaged hub icon 57
- color
 - alarms and warnings 88
 - map background, change 85
- colored ring 52, 60
- colors 88
- configuration files 109
- connections
 - delete 167
 - deleting 169
 - modifying 94
- contact data, modify 39
- copying map configurations 22
- Create Package 105
- customize the Network Map 83
- customizing your account 36

D

- data, delete 167
- date format, change 26
- default map configuration 21
- deleting connections 169
- device
 - adding 161
 - changing IP address 163
 - changing ports 163
 - changing priority 90
 - not seen 60
 - removing 160, 167
 - replacing 162
 - virtual devices 56
- Device Manager 147
 - changing default panel 26, 27, 37
 - linking from external site 176

- troubleshooting with 150
- device types 96
- device, disconnecting 21
- diamonds 57
 - approximate icon 57
 - logical view 58
 - LV unmapped icon 58
 - LV unmapped IP icon 58
 - shared port icon 58
 - unmapped IP icon 57
- disconnecting map session 21
- display, changing 87

E

- Element management 174
- e-mail
 - change account e-mail address 30
 - change your own e-mail address 39
 - test your e-mail address 41
- end node packages 103
- event filters 129
 - definition 131
 - delete 142
 - examples 133
 - list 142
 - modify 140
 - preparation 132
 - reset to defaults 143
- Events Browser 149
 - troubleshooting with 149
- Expiry 170

F

- find 75
- finding objects 75
- Fit Map to Window 86
- Fit Window to Map 86

G

- general thresholds 98
- grey background 60
- group drags 87

H

- Health Panel 53, 147

- aggregator 199
- Appliance Health report 49
- Exceptions report 49
 - troubleshooting with 148
- help format 27, 37
 - change 26
- help, Assistant window 27, 37
- Home Base 197
- Home page
 - aggregator 197

I

- icons
 - blue line under icons 61
 - change package icon 108
 - changing 91
 - changing size 85
 - locked 61
 - question mark 59
 - virtual devices 56
 - with colored ring 60
 - with grey background 60
- IP address
 - append to device labels 26, 36
 - changing in a device 163

L

- LEDs
 - colors 88
- licence, aggregator 191
- line alarm types 97
- Line Manager 147
 - default panel
 - changing 26
 - linking from external site 178
 - troubleshooting with 153
- line style, changing 84
- Lock 61, 106
- locked objects 61, 106
- Logical View
 - icon 58
- login
 - enabling 26
- long date format 27, 36
- LV Unmapped 58

LV Unmapped IP 58

M

map configuration 109
 allowing others to copy 26, 36
 change default 114
 copy 113
 copy permissions 26
 delete 113
 New 111
 open 112
 organizing 113
 Prime, saving 112
 rename 114
 restore Prime 115
 saving 110, 111
 sharing with other accounts 114
 map configuration, default 21
 map scale 53
 modem, modifying properties 122
 modifying connections 94
 MTBF 21
 resetting 164
 MTTR 21
 resetting 164
 multi-object packages 104, 105
 create manually 105
 MySQL ODBC Access 26

N

name of account 26, 36
 name, change for object 84
 Network Map 147
 autosave 111
 background color, change 85
 change icon 91
 changing the display 87
 changing the line style 84
 colored ring 60
 customizing 83, 93
 forcing object to be updated 94
 grey background 60
 icons, changing size 85
 modifying connections 94
 opening a configuration 112

placing an object at top 89
 purge 94
 question mark 59
 saving a map configuration 111
 starting a configuration 111
 Status Bar 53
 troubleshooting with 148
 view 85
 windows 84

NEWS

setting thresholds 98
 not seen device 60

O

objects
 change name 84
 find 75
 forcing to be updated 94
 placing at top of network 89

P

Pack command 104
 Package 105
 packaging 102
 change package icons 108
 map configuration files 109
 multi-object packages 105
 pager
 adding service providers 119
 change account information 30
 deleting service providers 127
 installing hardware 118
 listing service providers 120
 modifying modem properties 122
 modifying service providers 125
 test pager address 124
 testing 121
 testing pager number 125
 pager address
 change 39
 testing 42
 pager number
 change 39
 testing 42
 Pager Service Provider Configuration 117

- password
 - account, modifying 31
 - modify 40
 - Port Manager 147
 - changing default panel 27, 37
 - default panel
 - changing 26
 - linking from external site 177
 - troubleshooting with 153
 - Preferences
 - automatic packaging 107
 - colors 88
 - display 87
 - line style 84
 - map scale 85
 - may background color 85
 - Prime map configuration
 - restore 115
 - saving 112
 - priority
 - changing for device 90
 - Progress Bar 53
 - proxy services 203
 - default 204
 - via aggregator 207
 - via aggregator and remote appliance 209
 - via remote appliance 206
 - purge controls 170
 - purging objects 94
- Q**
- question mark 59
- R**
- Radio Cloud 57
 - regular account, description 19
 - remote appliances 192
 - list 196
 - restarting the appliance 16
 - ring, colored 60
- S**
- Save 110
 - Scale 86
 - scaling the map 85
 - Service Analyzer
 - Analyze button 73
 - introduction 72
 - service providers
 - adding 119
 - deleting 127
 - listing 120
 - modifying 125
 - Shared directory Access 26
 - Shared Port 58
 - short date format 27, 37
 - show icons 87
 - show outlines 87
 - shutdown the appliance 15
 - signal lights 88
 - status
 - allowing an account to receive e-mail 26
 - receive reports by e-mail 26
 - Status Bar 53
 - status reports
 - Appliance Health report 49
 - Exceptions 49
 - step line style 84
 - straight line style 84
- T**
- thresholds
 - alarm
 - changing 96
 - device 96
 - general 98
 - line alarms 97
 - Toolbar
 - aggregator 191
 - pull-down list 196
 - top of network 89
 - trash intervals 170
 - troubleshooting
 - samples 156
 - type of account, setting 26
 - types of account 17
- U**
- Unlock 61, 106
 - Unmanaged Hub 57

Unmapped IP 57

URL

 element management 174

 make visible 26, 36

user accounts, listing 24

V

vacation to-do list 185

virtual device, creating 96

virtual devices 56

 clouds 57

 diamonds 57

W

Web Access 26

Z

zigzag line style 84

zoom in or out in map display 85

