Peregrine

Network Discovery User Guide

Version 5.2

PART NO: DPND-52-EN02

Peregrine SYSTEMS®

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

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

This edition of the document applies to version 5.2 of the licensed program.

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

Contents

1 CHAPTER Welcome to Peregrine's Network 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 to manage your network.

See the *Reference Manual* for more detailed explanations of Network Discovery features.

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

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.

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

Licensing explained

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

Licenses are based on:

- how many devices and ports 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). Your license will handle 140 times as many attributes.

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 many functions are unavailable, so Network Discovery is unusable.

There are three ways to extend the time:

- Buy the product. You will receive a new production license.
- Clear the database.
- Receive another evaluation license.

Note: At the end of your evaluation period, you will still be able to see the Administration menus. You can request a new license by clicking **Administration** > **Appliance management** > **Generate licensing request**.

Note: If a Peregrine appliance in your network has an expired evaluation license, it cannot be aggregated. If you have more than one Peregrine appliance in your network, make sure you update your licenses for all appliances.

Logging in to Network Discovery

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 Peregrine appliance.

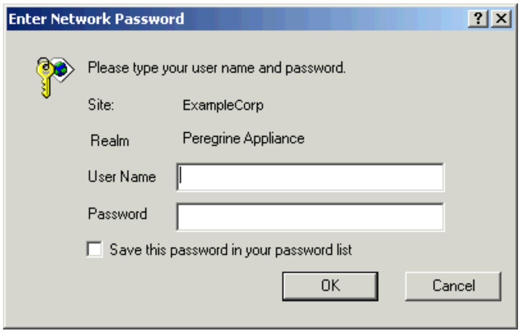
   When the connection is made, the Network Discovery splash screen appears, followed by the Login window.

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

Automation
Peregrine
Network Discovery® 5.2
Your Automation Solution
© 2004 Peregrine Systems, Inc. All rights reserved. This program is protected by U.S. and International Copyright laws.

Figure 1-2: Network Discovery Login Dialog



Enter Network Password

Please type your user name and password.

Site: ExampleCorp

Realm Peregrine Appliance

User Name

Password

☐ Save this password in your password list

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

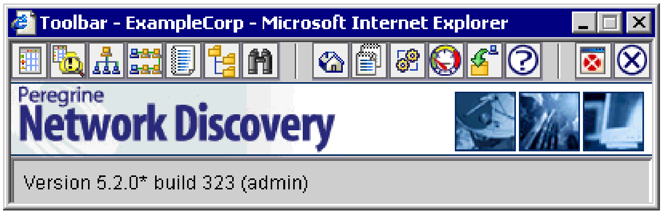
If your Network Discovery Administrator has not supplied you with an account and password, use the account name "demo" and the password "demo".

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 25.

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: Toolbar



Version 5.2.0* build 323 (admin)

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

Tip: Be sure to inform the people who clean and make repairs in the room where you keep your Peregrine appliance that it must be shut down properly.

Note: To shut down the Peregrine appliance safely when you are using the configuration interface, see the *Setup Guide*.

To shut down the Peregrine appliance—through the browser interface

1. Administration > Appliance management > Appliance Shutdown
2. Click **Shut down appliance.**

The Peregrine appliance shuts down safely.

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 5 minutes.

The web interface will provide status messages regarding the startup procedure.

2 User Accounts

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

There are five types of account:

- Demo
- IT Employee
- IT Manager
- Administrator
- Scanner

By default, Network Discovery has one of each type of account installed. If there are to be any other accounts, the owner of an Administrator account must create them.

Warning: In Network Discovery, all IT Manager and Administrator accounts have access to some powerful features. If you have an IT Manager or Administrator account, be careful not to overwrite the work of other IT Manager or Administrator accounts. In particular, Peregrine recommends that there be only one Network Discovery Administrator.

Table 2-1: Default accounts

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

Depending on your license, as many as 10 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.

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	✓	✓	✓	✓
Save any number of map configurations	✓	✓	✓	✓
Save a map configuration as Prime	—	—	✓	✓
Change a device icon	—	—	✓	✓
Change a package icon	✓	✓	✓	✓
Change a device’s priority	—	—	✓	✓
Change a device’s title or tag	—	—	✓	✓
Alarm Thresholds	view	view	view + change	view + change
Purge a device	—	—	✓	✓
Disconnect other accounts’ map sessions	—	—	—	✓
Managers (for example, Device Manager)				
View read and write community strings for device	—	—	✓	✓
View and use *set* link to MIB Browser	—	—	✓	✓
SNMP query default string	“public”	“public”	from Network Discovery	from Network Discovery
Update Model	—	—	✓	✓
Configure connections	—	—	✓	✓

Table 2-2: What the accounts can do

	Demo	IT Employee	IT Manager	Administrator
Break and force connections	—	—	✓	✓
MIB Browser				
Set SNMP variables	—	—	✓	✓
Read community string	—	view + edit	view + edit	view + edit
Write community string	—	—	view + edit	view + edit
Status				
View read and write community strings for network	—	—	✓	✓
Administration				
Change own password	—	✓	✓	✓
Configure own account	—	✓	✓	✓
Configure other accounts	—	—	—	✓
Manage own map configurations	—	✓	✓	✓
Copy map configurations from other accounts	—	✓	✓	✓
Select pager service provider	—	✓	✓	✓
Configure pager service provider	—	—	—	✓
Configure event filters	—	—	—	✓
Configure Peregrine appliance	—	—	—	✓
Configure network operations	—	—	—	✓
Access to shared directory	read	read	read	read/write

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
- View reports and appliance status

IT Employee accounts

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.

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

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
- Change device properties (title, tag, priority, and icon of a device)
- Change port properties
- 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
- 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

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

The default 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.

Scanner accounts

This type of account exists for one very specific purpose. The Scanner account can only upload scan files from Peregrine Desktop Inventory, and has no other administrative abilities.

For more information on the Scanner account, see *Using Network Discovery with Desktop Inventory and Desktop Administration*.

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

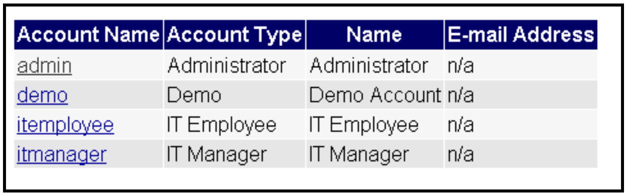
This page provides an alphabetical list of currently registered users, complete with their full name and e-mail address. The user names in the list are hyperlinked, so that you can click on the name and see all the options you can perform on that account.

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: In Network Discovery, all IT Manager and Administrator accounts have access to some powerful features. If you have an IT Manager or Administrator account, be careful not to overwrite the work of other IT Manager or Administrator accounts. In particular, Peregrine recommends that there be only one Network Discovery Administrator.

The account name must be 3–16 characters long. Acceptable characters are:

- a through z (must be lower case)
- 0 through 9

- hyphen (-) (the hyphen cannot be the first character in the account name)
- underscore (_) (the underscore cannot be the first character in the account name)

To add an account

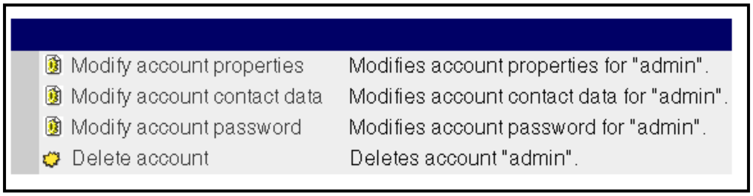
1 Click **Administration** > **Account administration** > **Add an account.**

2 Enter a login name.

3 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



Modify account properties	Modifies account properties for "admin".
Modify account contact data	Modifies account contact data for "admin".
Modify account password	Modifies account password for "admin".
Delete account	Deletes account "admin".

Customizing an account’s properties

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

Table 3-1: Account properties that 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). If chosen, an IP Address column will appear in the Alarm Viewer, Events Browser, and Service Analyzer.
Make URLs visible	Determines if hyperlinks are followed by the associated URL (for easy cut and paste).
Draw borders on tables in text mode	If you use the “as text” button, tables will have borders. Tables are easier to read with borders, but they take up more space on your screen.
Alternate colors in table rows	Tables are easier to read with alternating colors, but they take more space on your screen.
Highlight table rows on mouse over	Lets you highlight a row you want to look at.
Show navigation bar	Determines whether or not you see the navigation hyperlinks at the bottom of pages. The hyperlinks are the same as the buttons on the Toolbar.
Time before marking statistic as stale	Applies to Device Manager, Port Manager, Line Manager, Attribute Manager, Alarms Viewer, Health Panel, and Service Analyzer. When a statistic has not been updated for this set amount of time, the data will appear with a grey background.
Long date format	Determines how the date appears at the bottom of most panels and pages.
Short date format	Determines how the date appears 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.

Table 3-1: Account properties that Administrator accounts control

Property	Explanation
Default Device Manager panel	Determines which panel will appear when you open a Device Manager session.
Device Manager scan file viewer	Determines whether you will see a Java **Scan File Viewer**, or if you will download an xsf file, when you click the View **Scan Data** button in the Device Manager.
Default Port Manager panel	Determines which panel will appear when you open a Port Manager session.
Default Find panel	Determines which panel will appear when you open a Find session.
Default Attribute panel	Determines which panel will appear when you open an Attribute Manager session.
Default Device Manager Ports panel selection ■ increment	Determines which configuration will appear when you open a Ports panel in the Device Manager. ■ Determines how many rows of data the Ports panel displays at a time. Default: 24
Device Manager statistic	Statistic selected in the Device Manager Statistics panel.
Port Manager statistic	Statistic selected in the Port Manager Statistics panel.
Statistic interval	Interval selected for your Statistic panels in the Device Manager and Port Manager.
Statistic maximum	Statistic maximum selected for your Statistic panels in the Device Manager and Port Manager.
Statistic granularity	Statistic granularity selected for your Statistic panels in the Device Manager and Port Manager

To select an account for customizing

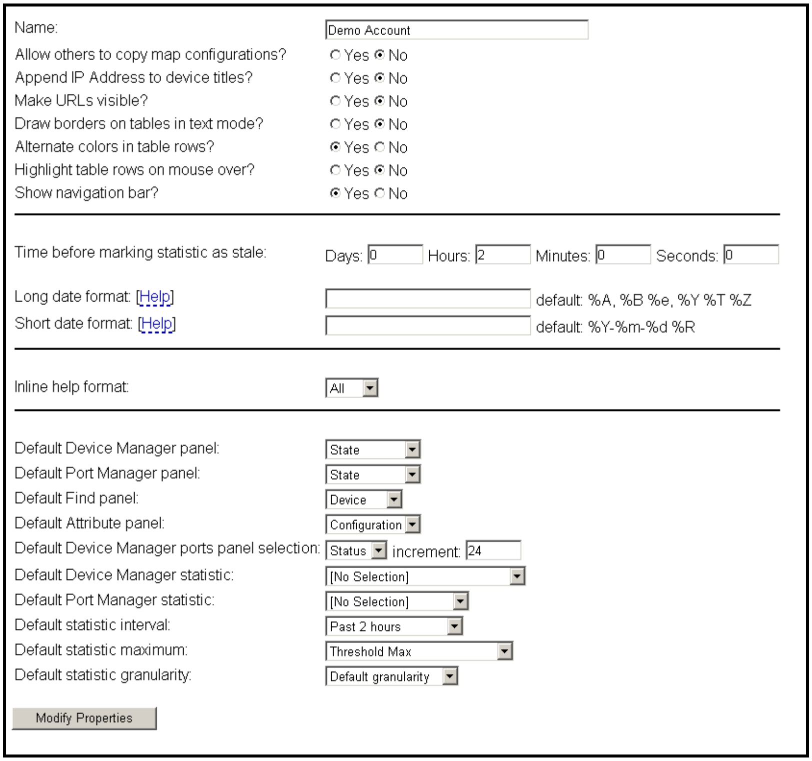
1. Click **Administration** > **Account administration** > **Account properties**.
2. Select an account from the list box.
3. Click **Modify Properties**.

To modify an account

1. *(optional)* Enter a descriptive name in the Name field.
2. Assign the appropriate properties.

3 Click **Modify Properties.**

Figure 3-3: Modify account properties



Name:	Demo Account
Allow others to copy map configurations?	○ Yes ● No
Append IP Address to device titles?	○ Yes ● No
Make URLs visible?	○ Yes ● No
Draw borders on tables in text mode?	○ Yes ● No
Alternate colors in table rows?	● Yes ○ No
Highlight table rows on mouse over?	○ Yes ● No
Show navigation bar?	● Yes ○ No
Time before marking statistic as stale:	Days: 0 Hours: 2 Minutes: 0 Seconds: 0
Long date format: [Help]	default: %A, %B %e, %Y %T %Z
Short date format: [Help]	default: %Y-%m-%d %R
Inline help format:	All
Default Device Manager panel:	State
Default Port Manager panel:	State
Default Find panel:	Device
Default Attribute panel:	Configuration
Default Device Manager ports panel selection:	Status increment: 24
Default Device Manager statistic:	[No Selection]
Default Port Manager statistic:	[No Selection]
Default statistic interval:	Past 2 hours
Default statistic maximum:	Threshold Max
Default statistic granularity:	Default granularity

Customizing an account's capabilities

You can change any of the account capabilities listed in the following table:

Account type	Determines the account's level of access to Network Discovery.
Web Access	Allows owner to use Network Discovery. You will probably enable this, but conceivably the user only needs MySQL ODBC access
MySQL ODBC Access	Allows owner of the account to export Network Discovery data to third-party data access applications to create custom reports.
Shared directory access	Allows owner of the account to access the shared directory. An Admin user can install updates and new licenses.
Password expiry	The number of days an account can be used before the password expires.

To select an account for customizing

1. Click **Administration** > **Account administration** > **Account capabilities.**
2. Select an account from the list box.
3. Click **Modify Capabilities.**

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.

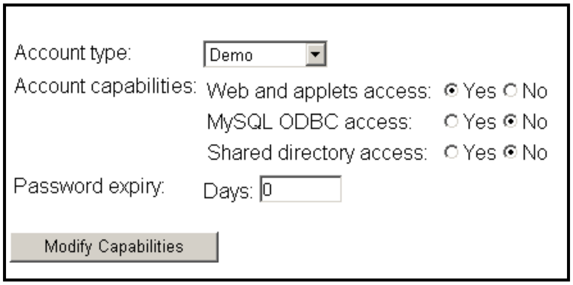
2. Determine what capabilities the account will have.

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

3. Change the appropriate capabilities.

4. Click **Modify Capabilities.**

Figure 3-4: Modify account capabilities



Account type: Demo

Account capabilities:
Web and applets access: ● Yes ○ No
MySQL ODBC access: ○ Yes ● No
Shared directory access: ○ Yes ● No

Password expiry: Days: 0

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.

To enable pager notification through an e-mail gateway

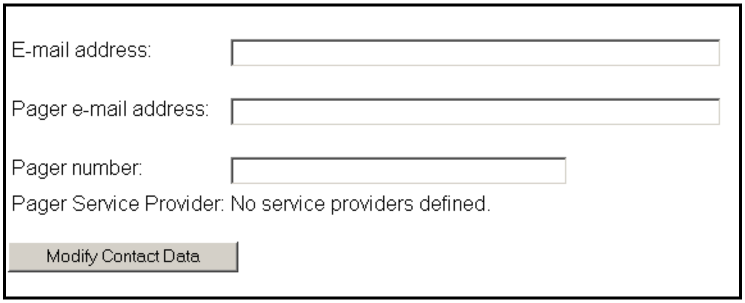
▶ Enter a pager address in the Pager e-mail address field.

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 137.

Figure 3-5: Modify contact data



E-mail address:

Pager e-mail address:

Pager number:

Pager Service Provider: No service providers defined.

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 (the minimum length depends on the setting at **Administration** > **Account administration** > **Appliance passwords**). 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.

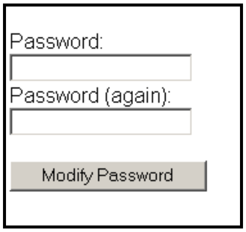
   Do not enter the current password (if any).
2. Enter the same new password in the second field.

   Entering the same password twice helps guard against typing errors.
3. Click **Modify Password**.

Note: Modifying the password resets the **Password Expiry** and **Failed Login Attempts** features.

Note: If the Administrator has set up the **Password History** feature, you cannot re-use passwords. You must have a new password each time you perform this procedure.

Figure 3-6: 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

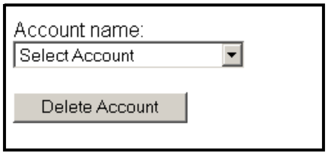
1. Click **Administration** > **Account administration** > **Delete an account**.

2. Select an account from the list box.
3. Click **Delete Account**.

To delete an account

▶ Click **Confirm**.

Figure 3-7: 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.

Setting the minimum password length

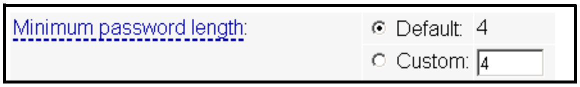
Your company may have a standard password length for all accounts in the organization. That standard may be different than the default password length in Network Discovery (which is 4-10 characters).

If your company requires you to have a different minimum password length, you can change Network Discovery so it is compliant with your standards.

To change the minimum password length

1. Click **Administration** > **Account administration** > **Appliance passwords.**
2. Enter a new number in the Custom text box.
3. Click **Change.**

Figure 3-8: Minimum password length



Minimum password length:
● Default: 4
○ Custom: 4

Setting the number of failed login attempts

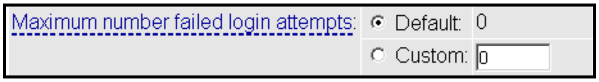
As a security feature, the Administrator can define how many times an account can try to login to Network Discovery.

If the user cannot login, and this threshold has been passed, the account will be locked out until the Administrator changes the account password (see *Modifying an account password* on page 33).

To change the maximum number of failed login attempts

1. Click **Administration** > **Account administration** > **Appliance passwords.**
2. Enter a new number in the Custom text box.
3. Click **Change.**

Figure 3-9: Maximum number of failed login attempts



Maximum number failed login attempts:
● Default: 0
○ Custom: 0

Setting the password history

For security purposes, users should change their passwords often. To increase security, this feature ensures that users use different passwords, rather than re-using the same passwords over and over again. For example, if you set this to “5,” a user must use a new, unique password the next 5 times he/she changes his/her password.

The **Delete password history** feature determines how long Network Discovery keeps a record of the passwords used by each account. When this time expires, an user will be able to re-use an old password.

Note: Delete password history always takes precedence. If you surpass the set Password History limit, you cannot reuse a password until the Delete password history time has expired.

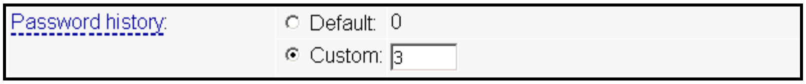
To set the password history

1 Click **Administration** > **Account administration** > **Appliance passwords.**

2 Enter a new number in the Custom text box.

3 Click **Change.**

Figure 3-10: Password history



Password history: ○ Default: 0
● Custom: 3

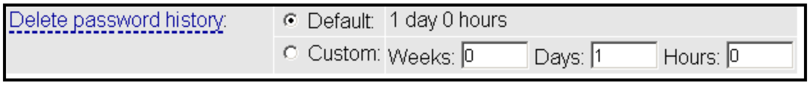
To delete the password history

1 Click **Administration** > **Account administration** > **Appliance passwords.**

2 Set a time for the password history to be deleted.

3 Click **Change.**

Figure 3-11: Delete password history



Delete password history: ● Default: 1 day 0 hours
○ Custom: Weeks: 0 Days: 1 Hours: 0

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

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: You can see a complete list of the properties on page 28. Many of these properties will be of more interest to you when you are more experienced with Network Discovery.

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.**

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 137.

3. Click **Modify Contact Data**.

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.

Note: Passwords are case-sensitive. “Magic”, “MAGIC”, and “magic” are different passwords

Passwords can be up to 20 characters long (the minimum length depends on the setting at **Administration** > **Account administration** > **Appliance passwords**). 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. You will also need to close the Toolbar and open it again, so the applets receive the new password.

Note: If the Administrator has set up the **Password History** feature, you cannot re-use passwords. You must have a new password each time you perform this procedure.

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**.

If you do not receive the message, it could be because:

- no e-mail address is provided
- an incorrect e-mail address is provided
- a mail server has not been specified for use with Network Discovery
- the Network Discovery mail server is not working
- the receiving mail server is not working

Testing your pager address

Testing your pager address will send a 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 a message to your pager, click **Confirm**.

If you do not receive the page, it could be because:

- incorrect pager data is provided in the pager service provider profile
- no pager data is provided in your account profile
- incorrect pager data is provided in your account profile
- no external modem is connected to the Peregrine appliance
- the external modem connected to the Peregrine appliance is turned off
- there are modem synchronization problems
- there is no dial tone on the phone line being used
- your service provider is having problems
- your pager is turned off

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**.

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

- incorrect pager data is provided in the pager service provider profile
- no pager data is provided in your account contact data
- no service provider profile is specified in your account contact data
- incorrect pager data is provided in your account contact profile
- no external modem is connected to the Peregrine appliance
- the external modem connected to the Peregrine appliance is turned off
- there are modem synchronization problems
- there is no dial tone on the phone line being used
- your service provider is having problems
- your pager is turned off

CHAPTER 5 A Tour: Toolbar, Health Panel, Alarms Viewer, Network Map

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

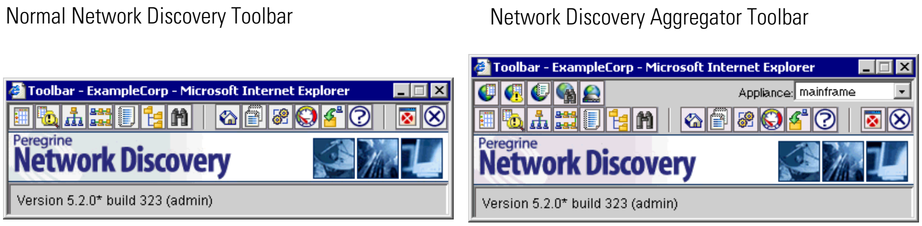
Topics in this chapter include:

The Toolbar is the starting point

The Toolbars and buttons

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. You may see one of two possible Toolbars:

Figure 5-1: Normal and Aggregator Toolbars



Normal Network Discovery Toolbar

Network Discovery Aggregator Toolbar

Toolbar - ExampleCorp - Microsoft Internet Explorer
Peregrine
Network Discovery
Version 5.2.0* build 323 (admin)
Toolbar - ExampleCorp - Microsoft Internet Explorer
Appliance: mainframe
Peregrine
Network Discovery
Version 5.2.0* build 323 (admin)

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

For more information on the Network Discovery Aggregator, see *Chapter 15, Using an Aggregator*.

The difference between an Aggregator Toolbar and a single-appliance Toolbar is immediately visible: the Aggregator Toolbar has an extra row of buttons on top. The rest of the Aggregator Toolbar works exactly as the single-appliance Toolbar does.

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

The first group of buttons controls Aggregator features:

Aggregate Health Panel	Opens the Aggregate Health Panel.
Aggregate Alarms Viewer	Opens the Aggregate Alarms Viewer.
Aggregate Events Browser	Opens the Aggregate Events Browser.
Aggregate Find	Opens the Aggregate Find.
Remote Appliances	Lists the Peregrine appliances that can be viewed remotely and may be supplying data to the Aggregate Health Panel.

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

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

The Aggregator appliance is listed at the top, using its system name. An asterisk appears after the system name to indicate that this is the Aggregator.

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

Health Panel	Opens the Health Panel.
Alarms Viewer	Opens the Alarms Viewer.
Network Map	Opens the Network Map window.
Service Analyzer	View end-to-end network performance.
Events Browser	View recent events.

MIB Browser	Opens the MIB Browser.
Find	Search for devices and ports of devices.

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

Home/ Home Base	Home is the home page for a single appliance. Home Base is the home for the Aggregator appliance.
Reports	View network statistics.
Administration	The function of this button depends on your account. ■ Demo users have no access to administration. ■ IT Employee users: Configure own account. ■ IT Manager: Configure own account ■ Administrator users: - Perform initial setup - Set appliance system variables - Configure own and other accounts - Set appliance system variables - Set up Network Discovery
Status	View configuration of the Peregrine appliance and of Network Discovery.
Download	Allows downloading of components for Windows.
Help	Read documentation. This menu includes all manuals, release notes, and some quick-reference windows.

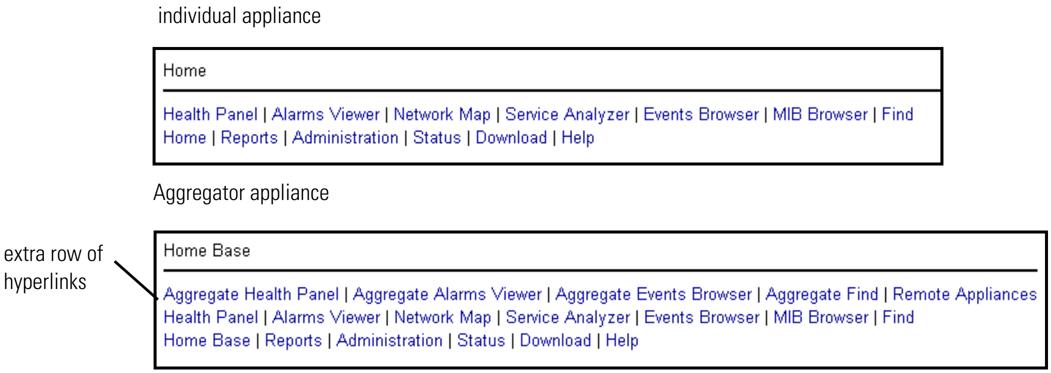
The fourth group of buttons controls your web browser environment.

☒	Close	Close all Network Discovery windows (for an Aggregator, closes all the windows for the selected Peregrine appliance).
⊗	Exit	Quit Network Discovery completely, but leaves any active web browser windows open.

Navigating with buttons and links

The Toolbar 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: Differences in navigation bars



Home

Health Panel | Alarms Viewer | Network Map | Service Analyzer | Events Browser | MIB Browser | Find
Home | Reports | Administration | Status | Download | Help

Home Base

Aggregate Health Panel | Aggregate Alarms Viewer | Aggregate Events Browser | Aggregate Find | Remote Appliances
Health Panel | Alarms Viewer | Network Map | Service Analyzer | Events Browser | MIB Browser | Find
Home Base | Reports | Administration | Status | Download | Help

There is an extra row of hyperlinks. The extra (top) row affects the Aggregator appliance. The new hyperlinks are “Aggregate Health Panel”, “Aggregate Alarms Viewer”, “Aggregate Events Browser”, and “Remote Appliances.”

For more information on the Aggregator, see *Chapter 15, Using an Aggregator*.

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

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.

Network Discovery: an integrated approach

There are many ways to look at your network data with Network Discovery. The Health Panel, the Network Map, and the Alarms Viewer to see your devices, and to determine the devices that currently have problems.

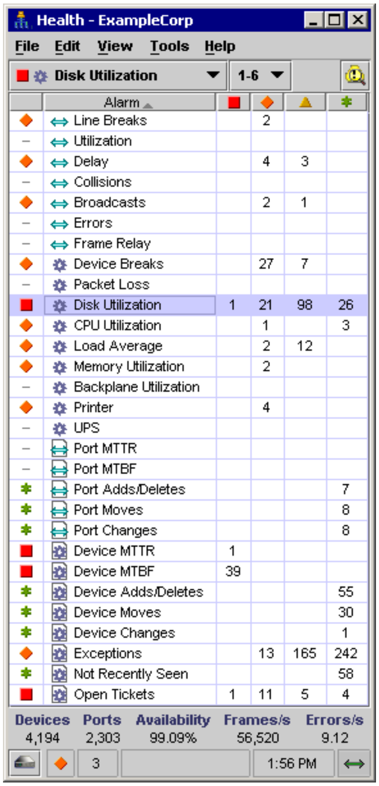
Typically, a user would start with the Health Panel and Network Map. The Health Panel lists all the alarms currently on your network, whereas the Network Map shows a graphical representation of the network layout. To see a list of devices with these alarms, double-click on an alarm category in the Health Panel, and the Alarm Viewer opens.

The Alarms Viewer shows all the devices on the network with current alarms. From the Alarms Viewer, you can double click on an alarm and open up a Device Manager, and from there you can investigate a problem with that device.

See a network overview with the Health Panel

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

Figure 5-3: Health Panel example (all alarm categories shown)



	Alarm	🟥	◆	▲	✱
◆	Line Breaks		2		
–	Utilization				
◆	Delay		4	3	
–	Collisions				
◆	Broadcasts		2	1	
–	Errors				
–	Frame Relay				
◆	Device Breaks		27	7	
–	Packet Loss				
🟥	Disk Utilization	1	21	98	26
◆	CPU Utilization		1		3
◆	Load Average		2	12	
◆	Memory Utilization		2		
–	Backplane Utilization				
◆	Printer		4		
–	UPS				
–	Port MTTR				
–	Port MTBF				
✱	Port Adds/Deletes				7
✱	Port Moves				8
✱	Port Changes				8
🟥	Device MTTR	1			
🟥	Device MTBF	39			
✱	Device Adds/Deletes				55
✱	Device Moves				30
✱	Device Changes				1
◆	Exceptions		13	165	242
✱	Not Recently Seen				58
🟥	Open Tickets	1	11	5	4

Devices	Ports	Availability	Frames/s	Errors/s
4,194	2,303	99.09%	56,520	9.12

◆ 3 1:56 PM

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

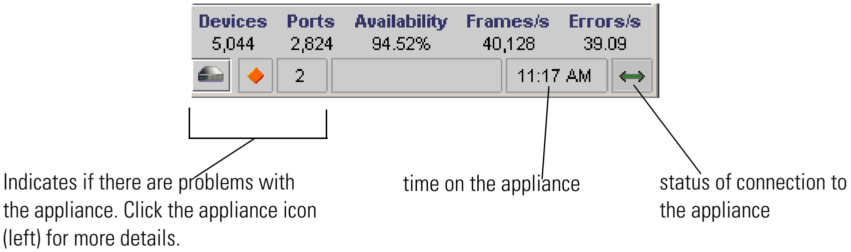
There are icons on the Health Panel to distinguish device and port alarms. The Health Panel is divided into four sections as indicated by these icons:

Category	Indicator
Port Attribute Alarm	↔
Device Attribute Alarm	⚙
Port Report Alarm	🗎↔
Device Report Alarm	🗎⚙

The Health Panel will show you how many alarms are on your network. You can drill down with the Alarms Viewer to see exactly which devices have the alarms.

Note: The Aggregate Health Panel works the same way as the normal Health Panel, but it shows information for all the Peregrine appliances in your network. For more information, see *Using the Aggregate Health Panel* on page 206.

Figure 5-4: Health Panel statistics and Appliance Health Data



Devices	Ports	Availability	Frames/s	Errors/s
5,044	2,824	94.52%	40,128	39.09

2 · 11:17 AM

Indicates if there are problems with the appliance. Click the appliance icon (left) for more details.

time on the appliance

status of connection to the appliance

Statistic	Explanation
Devices	The number of discovered devices in the network.
Ports	The number of discovered ports in your network
Availability	This number represents the number of real devices with priority 3 (or higher) that are operational as a percentage of the total number of real 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.

Customizing the Alarm List

You can change the appearance of the Health Panel so you see only the alarms in which you are interested.

To customize the alarms seen on the Health Panel:

1. From the Health Panel, click **Edit** > **User Preferences** > **Health Panel** tab.

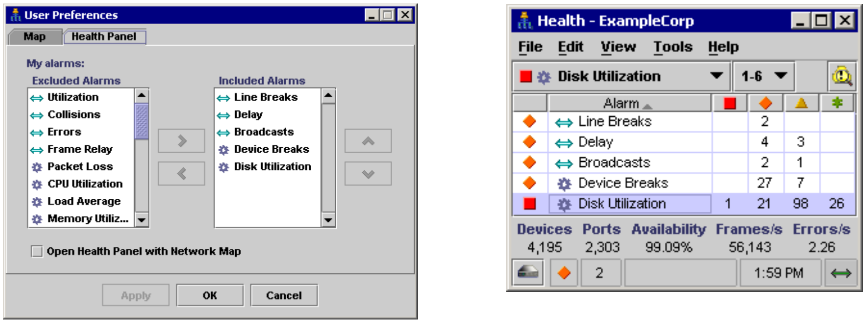
   Here, you can create a list of the alarms you want to see on the Health Panel.

2. After you have created your list, click **Apply**.
3. Click **OK**.

   Next, you must apply these changes in the View menu.

4 Click View > My User Alarms Only.

Figure 5-5: Health Panel Preferences



Setup in **Edit** > **User Preferences** > **Health Panel tab**

User Preferences

My alarms:

Excluded Alarms	Included Alarms
Utilization	Line Breaks
Collisions	Delay
Errors	Broadcasts
Frame Relay	Device Breaks
Packet Loss	Disk Utilization
CPU Utilization	
Load Average	
Memory Utiliz...	

☐ Open Health Panel with Network Map

Result with **View** > **My User Alarms Only**

Health - ExampleCorp

	Alarm	🟥	◆	▲	✱
◆	Line Breaks		2		
◆	Delay		4	3	
◆	Broadcasts		2	1	
◆	Device Breaks		27	7	
🟥	Disk Utilization	1	21	98	26

Devices	Ports	Availability	Frames/s	Errors/s
4,195	2,303	99.09%	56,143	2.26

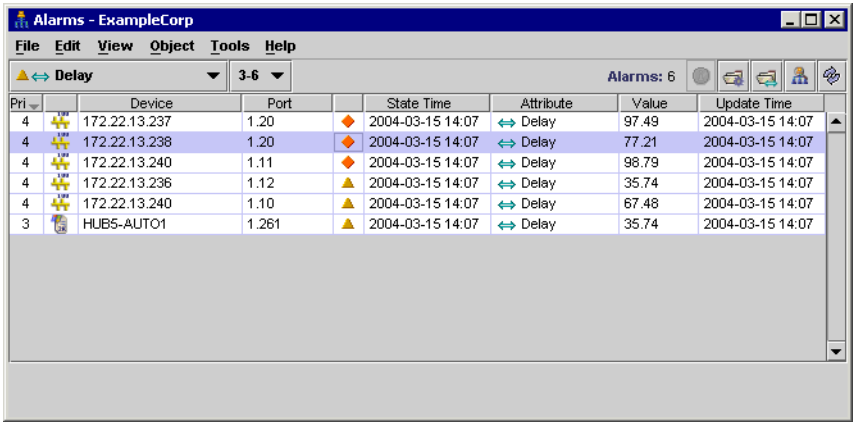
◆ 2 1:59 PM

Using the Alarms Viewer

The Alarms Viewer is an extension of the Health Panel, and shows you exactly on which devices and ports the alarms have occurred.

By double-clicking on a line in the Health Panel, you will open the Alarms Viewer. The Alarms Viewer works with the Health Panel to show you which devices on your network have Critical, Major, Minor, or Info alarms.

Figure 5-6: Alarms Viewer



Pri		Device	Port		State Time	Attribute	Value	Update Time
4		172.22.13.237	1.20	◆	2004-03-15 14:07	⇔ Delay	97.49	2004-03-15 14:07
4		172.22.13.238	1.20	◆	2004-03-15 14:07	⇔ Delay	77.21	2004-03-15 14:07
4		172.22.13.240	1.11	◆	2004-03-15 14:07	⇔ Delay	98.79	2004-03-15 14:07
4		172.22.13.236	1.12	▲	2004-03-15 14:07	⇔ Delay	35.74	2004-03-15 14:07
4		172.22.13.240	1.10	▲	2004-03-15 14:07	⇔ Delay	67.48	2004-03-15 14:07
3		HUB5-AUTO1	1.261	▲	2004-03-15 14:07	⇔ Delay	35.74	2004-03-15 14:07

The status bar in the Alarms Viewer is similar to that on the Health Panel. You can change the displayed alarm type or priority with the pull-down lists on either window. Your selection will appear in the Health Panel, Network Map and the Alarms Viewer.

Note: The Alarms Viewer will show a maximum of 1000 alarms.

Saving data to a text file

You can now use the **Save Table Data** feature to save selected info into a text (.tsv) file in the following Network Discovery features:

- Health Panel
- MIB Browser
- Find
- Alarms Viewer
- Service Analyzer
- Events Browser

You can save the entire contents of a window, or you can Ctrl-click to select the data you want to save.

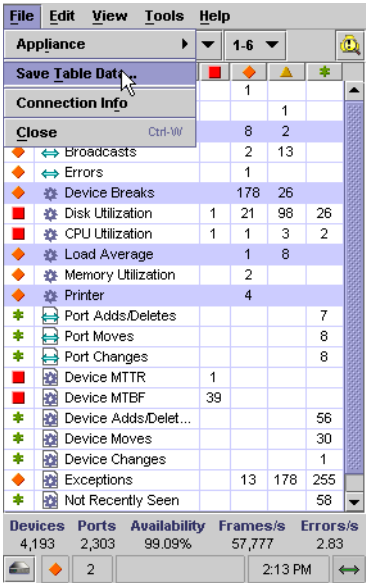
Saving data to a text file

1. Select the table items you want to save. To select the entire table, click **Edit** > **Select Table.**
2. Click **File** > **Save Table Data.**

   A Save Table Data dialog appears.
3. Select a file name and location for the text files.

4 Click Save.

Figure 5-7: Example: saving the Health Panel data to a text file



			🟥	◆	▲	✚
				1		
					1	
				8	2	
◆	⇔	Broadcasts		2	13	
◆	⇔	Errors		1		
◆	⚙	Device Breaks		178	26	
🟥	⚙	Disk Utilization	1	21	98	26
🟥	⚙	CPU Utilization	1	1	3	2
◆	⚙	Load Average		1	8	
◆	⚙	Memory Utilization		2		
◆	⚙	Printer		4		
✚		Port Adds/Deletes				7
✚		Port Moves				8
✚		Port Changes				8
🟥	⚙	Device MTTR	1			
🟥	⚙	Device MTBF	39			
✚	⚙	Device Adds/Delet...				56
✚	⚙	Device Moves				30
✚	⚙	Device Changes				1
◆	⚙	Exceptions		13	178	255
✚	⚙	Not Recently Seen				58

Devices	Ports	Availability	Frames/s	Errors/s
4,193	2,303	99.09%	57,777	2.83

◆ 2 2:13 PM

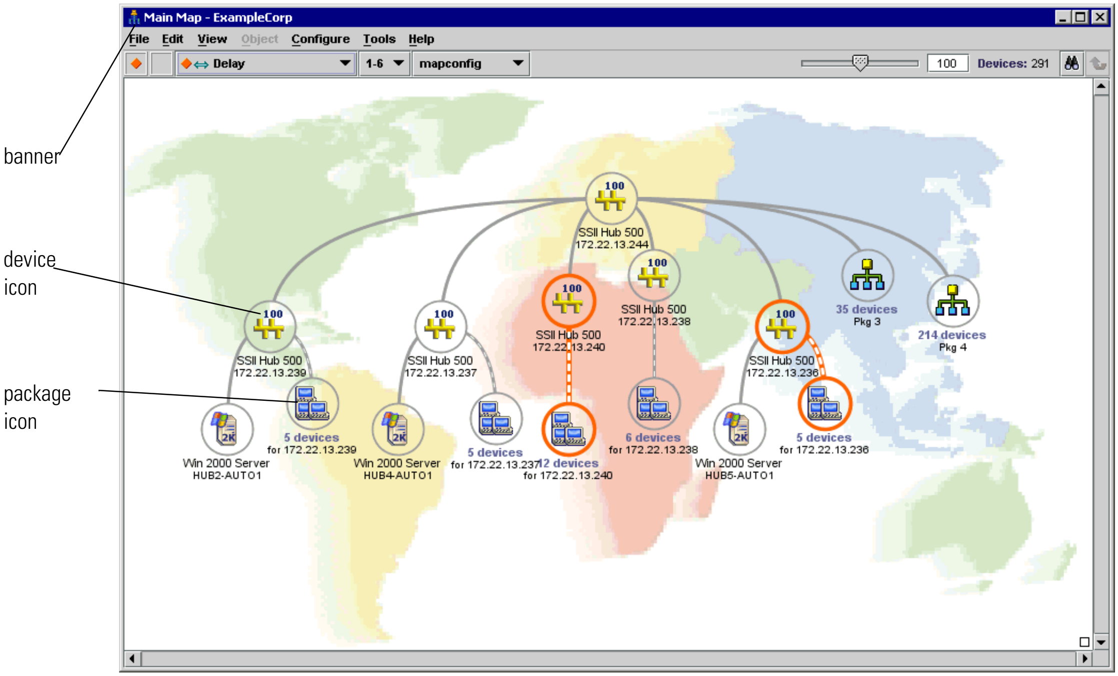
The Network Map provides a graphical view

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.

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

Figure 5-8: Network Map



To determine what the Map will display, select an alarm category on the Health Panel or click the alarm list on the map status bar.

The colored ring around an icon indicates the device's status for the category you select. For example, if you select Device MTBF, the devices that have critical alarms for their Mean Time Between Failures will have red rings and the devices that have minor alarms will have gold rings.

Note: To show rings the objects must be within the priority range as selected on the map status bar, Health Panel, or Alarms Viewer. (Information about setting device priorities is in *Changing Device Properties* on page 110.)

Note: Devices and ports that do not have applicable attribute or report data will not have a ring (for example, virtual devices).

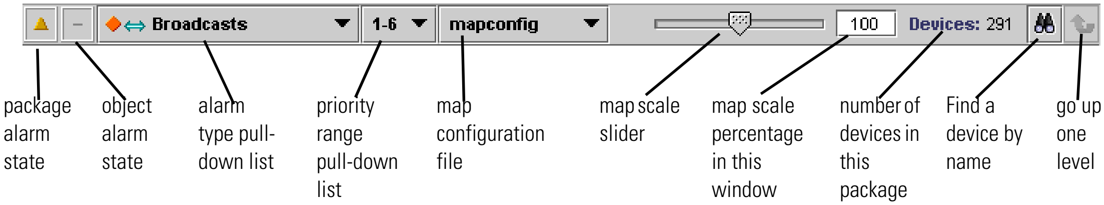
Status Bar

The Status Bar appears at the top 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.

Figure 5-9: Network Map Status bar



What are the icons on the map?

The Icons

Network Discovery tries to develop a realistic view of your network, and that view is represented with icons (representing devices or groups of devices) and lines that connect the devices.

Network Discovery selects device icons based on the data collected from that device. For example, if Network Discovery sees that a device is a Microsoft Windows 2000 workstation, that device will appear on the map with a “Win2000 Workstation” icon.

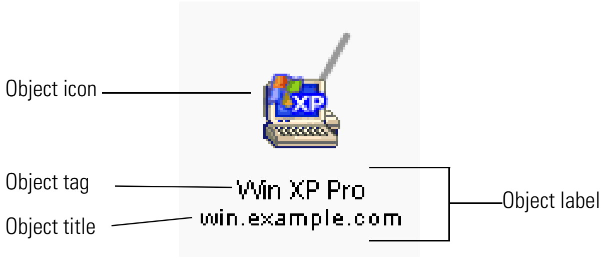
Note: Network Discovery will usually select the correct device icon. If for some reason, the wrong icon has been selected, you can change it. See *Chapter 7, Customizing Your View of the Network Map*.

Once you understand the map, you can make changes to its look and organization. Later in the *User Guide*, you will read about packaging, map configuration files, etc. This section will teach you what the different icons represent.

The icons on the map fall into categories:

Icon Type	Description
Device Icons	Device icons represent the physical equipment in your network. To understand the difference between real devices and virtual devices, see the *Reference Manual*.
Package Icons	A package is a collection of objects (objects means either devices or packages) that is represented by an icon.

Figure 5-10: Icon terms



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.

For more information on the real and virtual devices, see the *Reference Manual*.

You can see a complete list of all the icons used in Network Discovery in **Help** > **Classifications** > **Device Types/Package Types**.

The object label

For devices, the object label tells you what kind of device it is. For packages, the object label tells you how many devices are within the package.

Real device

- device tag further classifies the device (classification is begun by the device icon)
- device title identifies a specific device

Table 5-1: Device tag classes

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

[a] Limited information is available, or, a managed device is not listed in the Network Discovery Rulebase; see also Table 5-2.

Table 5-2: Device tag endings

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

Virtual device

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

Package

- package tag shows number of devices contained by package
- package title can identify parent device (automatic package) or top object of package (multi-object package); can also be arbitrary (any package)

The priority

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

By default, priorities 5 and 6 are reserved for the user. By default, priority 6 is reserved for those devices that should trigger event notification—see *Setting up Event Filters* on page 147.

The top object

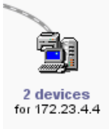
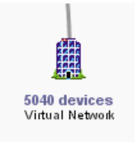
Whether a given object is the top object in the window or not is a property of the window, not of the object.

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

To make an object the “top object,” see *Placing an object at the top of the map window* on page 107.

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:

Package Type	Description	Example
Automatic Package	These packages are automatically created by Network Discovery.	
Multi-object Package	These packages are created by the user, and can contain any devices you wish to place in them. For more information on packaging, see *Packaging Your Network* on page 117.	

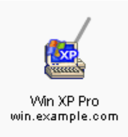
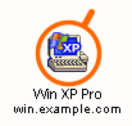
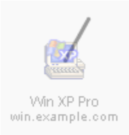
Any map window can contain packages. You can modify the contents of a package (selecting objects or groups of objects) exactly as you can in the Main Map.

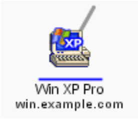
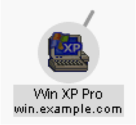
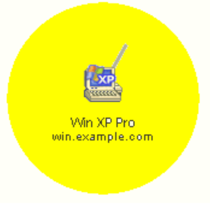
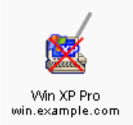
As with other icons, you will sometimes see package icons with colored rings around them (when you select an alarm type). The color of the ring around the package depends on the color of rings around objects inside the package. The ring around the package icon will match the most severe instance of its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

For example, if there are Critical (red), Minor (gold) and Info (green) rings inside a package, the package will have a Critical (red) ring.

Icon Appearance

The following table shows a device icon in the possible states as it will appear on the Network Map.

Appearance	What it means
 Win XP Pro win.example.com	**Normal Icon** This is how a device icon will appear when: ■ no alarms are selected ■ an alarm has been selected but that type of alarm does not apply to this device ■ an alarm has been selected but this device is not in the priority range
 Win XP Pro win.example.com	**Colored Ring** A thin gray ring will appear around a device when: ■ this device is in the priority range ■ this device is not alarmed A colored ring will appear around a device when: ■ an alarm is selected that exists on this device ■ this device is in the priority range **Note:** In the case of packages, the package icon can have a colored ring that represents the highest alarm state of the devices contained in that package.
 Win XP Pro win.example.com	**Faded Icon** If an object appears faded, that means Network Discovery has not seen that device for more than 24 hours. Network Discovery will eventually deactivate such a device from the Network Map and, eventually, Network Discovery will purge the device and all its associated data.

Appearance	What it means
	**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 (**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 117.
	**Selected Icon** If you select an icon on the Network Map, it will appear dark.
	**Found Icon** This icon was located on the Network Map using the Locate feature. **Note:** For packages, the large yellow circle indicated that you have just left this package, as you are navigating through the Network Map. Also note that the package tag is a different color after you have been inside the package.
	**Deactivated or Hidden Icon** This device has been manually deactivated or hidden by an Admin account.

Access to the Network Map

These commands control your Network Map session.

Disconnect

From any map window, click **File** > **Disconnect**.

This command suspends your map session without closing map windows or saving your configuration file. This is a good way to free up a map session for use by another account.

Use the **Disconnect** command if you want to:

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

Note: Once you disconnect, map windows become static. Alarms are displayed but will not be updated until you **Reconnect**. You can change the display of open map windows but not the contents (such as packaging).

Table 5-3: Effects of Disconnect command on Network Map

Class of tasks	Effect
Tasks that work the same	printing a map window
	scaling a map window
	scrolling a map window
	opening a Device Manager window
Tasks that work differently	moving an object in open map windows (object may not stay in position)

Table 5-3: Effects of Disconnect command on Network Map (Continued)

Class of tasks	Effect
Tasks you cannot perform	opening a map window
	opening a package
	packaging / unpackaging objects
	saving / opening a configuration file

Note: Always **Save** your map configuration before you **Disconnect**.

Reconnect

From any map window, click **File** > **Reconnect**.

The **Reconnect** command re-establishes and resumes your map session after a disconnection.

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

Use the **Reconnect** command if you want to:

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

Each time you click the **Reconnect** command, Network Discovery makes several attempts to reconnect, not just one. Network Discovery will attempt to reconnect continually for up to an hour until successful.

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

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

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

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

Close

From any map window, click **File** > **Close**.

This command closes the current map window.

Close Map

From any map window, click **File** > **Close Map**.

This command closes all map windows and ends the map session.

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

The **Close Map** command ends the map session, but:

- Manager windows are left open.
- The name of the current map configuration is stored (so that the configuration can be loaded automatically the next time you open a Network Map).
- If you are using the Forecast feature, the map is returned to the present (for more information on Forecast, see *Checking the Network Forecast* on page 72).

Checking the Network Forecast

The Forecast feature predicts how the network will perform in the future. From any map window, click **Tools** > **Forecast**, and select a future point to see. You can choose 1, 2, 3, 6, 9, or 12 months into the future.

Once you select a Forecast time period, Network Discovery computes a probable view of the Health Panel, Network Map, and Alarms Viewer based on existing data.

Important: When calculating Forecast statistics, Network Discovery assumes that no physical changes will be made to the network.

Forecast data is not calculated for all network alarms. Network Discovery only predicts the future state of some alarm categories (see the complete list at **Help** > **Classifications** > **Supported Device/Port Attributes**).

Note: When Forecast mode is on, the Health Panel will only show these alarm categories. Also, the alarm pull-down list in the Health Panel, Alarms Viewer, and Network Map will show these alarm categories.

To estimate future performance of these alarm categories, Network Discovery records their peak values every day. Those daily peak values are calculated and averaged, and Network Discovery will predict future values based on the pattern of past values. This is helpful because Network Discovery can extend its predictions and estimate at which point an attribute will reach an alarm threshold. You will be able to see approximately when an alarm will occur on a device.

As an example, consider Disk Utilization on a backup server. You could be backing up your data every day. The Disk Utilization graph will show the steady increase of saved data. Using the Forecast feature will show you if the server hard disk will reach an alarmable threshold in the future.

Note: For Forecast to work, there must be at least 21 days of data. The data is stored as long as the device is present in the network.

While using the **Forecast** command, some controls or display areas in a window are indicated by a pale green background. Also:

- The pop-ups on the Network Map will not show ServiceCenter ticket information
- only future alarms that can be predicted are shown on the Health Panel.
- “Forecast” is shown at the bottom of the Health Panel.

Related to the Forecast feature, you can also see predictions of future performance in the Statistics panel of the Device Manager and Port Manager. In the pull-down list, you can select items such as “Past + Next 30 days” which will give you a visual indication of how the attribute has performed recently, and how it may perform in the future.

For more information, see the Device Manager section of the *Reference Manual*.

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

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

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 Service Analyzer, or through hyperlinks available in other features.

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

For detailed information on the Device Manager, see the *Reference Manual*.

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, or double-click on a line on the Network Map.

For detailed information on the Port Manager, see the *Reference Manual*.

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** > **Classifications** > **Supported Device/Port Attributes**.

To open the Attribute Manager for a device

1. Open a Device Manager, or Line Manager.
2. Select the State button.
3. In the **Attribute Name List**, click an Attribute name.

To open the Attribute Manager for a port

▶ Click an **Attribute Name** from one of the following:

  - the Device Manager
  - the Port Manager
  - the Line Manager
  - the Service Analyzer

For detailed information on the Attribute Manager, see the *Reference Manual*.

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

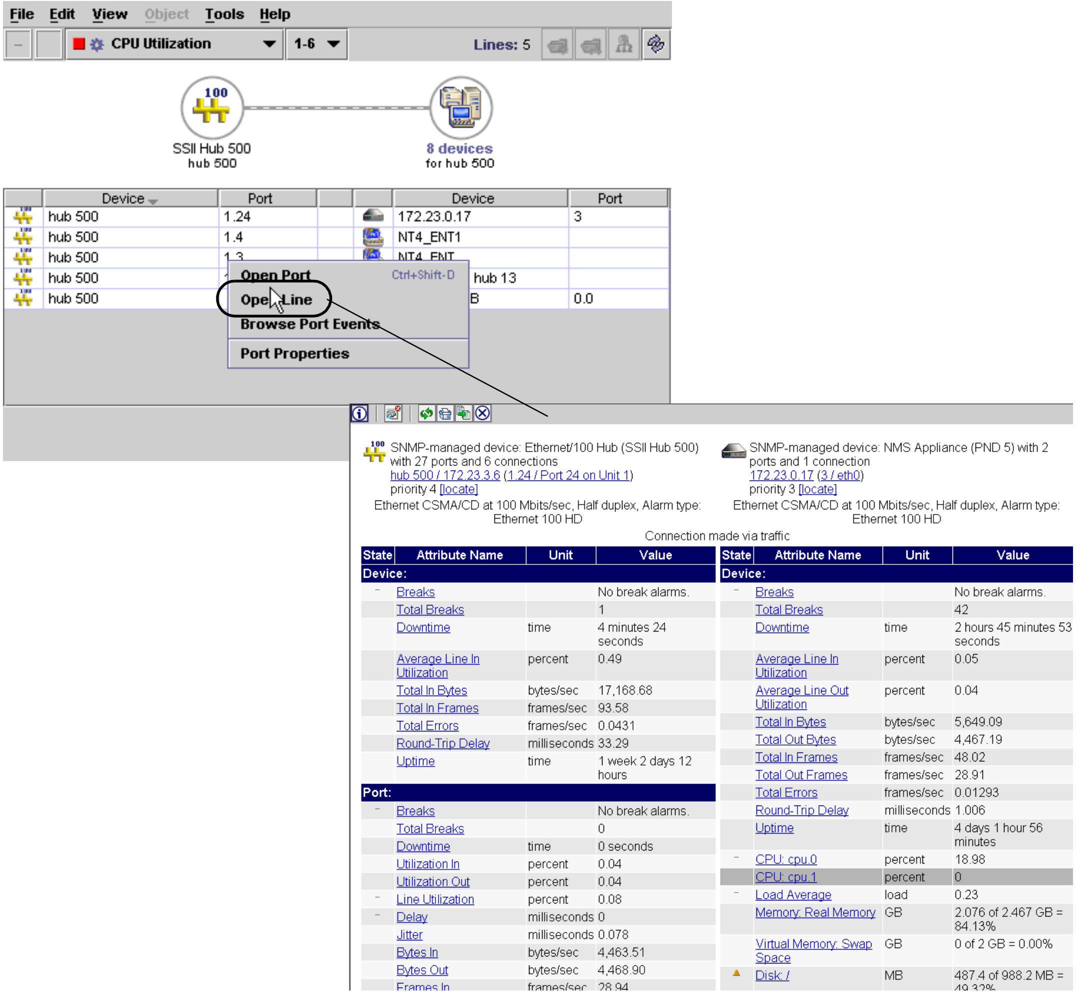
If you open a Multiple Line Manager, it appears as shown in Figure 6-1. To open a Single Line Manager, right-click on one of the ports and select **Open Line**.

You can use the hyperlinks on the Single Line Manager to 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.

For detailed information on the Line Manager, see the *Reference Manual*.

Figure 6-1: Right-click on a port number in the Multiple Line Manager



Device	Port	Device	Port
hub 500	1.24	172.23.0.17	3
hub 500	1.4	NT4_ENT1	
hub 500	1.3	NT4_ENT	
hub 500	1	hub 13	
hub 500		B	0.0

SNMP-managed device: Ethernet/100 Hub (SSII Hub 500) with 27 ports and 6 connections
hub 500 / 172.23.3.6 (1.24 / Port 24 on Unit 1)
priority 4 [locate]

Ethernet CSMA/CD at 100 Mbits/sec, Half duplex, Alarm type: Ethernet 100 HD

SNMP-managed device: NMS Appliance (PND 5) with 2 ports and 1 connection
172.23.0.17 (3 / eth0)
priority 3 [locate]

Ethernet CSMA/CD at 100 Mbits/sec, Half duplex, Alarm type: Ethernet 100 HD

Connection made via traffic

State	Attribute Name	Unit	Value
Device:			
−	Breaks		No break alarms.
	Total Breaks		1
	Downtime	time	4 minutes 24 seconds
	Average Line In Utilization	percent	0.49
	Total In Bytes	bytes/sec	17,168.68
	Total In Frames	frames/sec	93.58
	Total Errors	frames/sec	0.0431
	Round-Trip Delay	milliseconds	33.29
	Uptime	time	1 week 2 days 12 hours
Port:			
−	Breaks		No break alarms.
	Total Breaks		0
	Downtime	time	0 seconds
	Utilization In	percent	0.04
	Utilization Out	percent	0.04
−	Line Utilization	percent	0.08
−	Delay	milliseconds	0
	Jitter	milliseconds	0.078
	Bytes In	bytes/sec	4,463.51
	Bytes Out	bytes/sec	4,468.90
	Frames In	frames/sec	28.94

State	Attribute Name	Unit	Value
Device:			
−	Breaks		No break alarms.
	Total Breaks		42
	Downtime	time	2 hours 45 minutes 53 seconds
	Average Line In Utilization	percent	0.05
	Average Line Out Utilization	percent	0.04
	Total In Bytes	bytes/sec	5,649.09
	Total Out Bytes	bytes/sec	4,467.19
	Total In Frames	frames/sec	48.02
	Total Out Frames	frames/sec	28.91
	Total Errors	frames/sec	0.01293
	Round-Trip Delay	milliseconds	1.006
	Uptime	time	4 days 1 hour 56 minutes
−	CPU: cpu.0	percent	18.98
	CPU: cpu.1	percent	0
−	Load Average	load	0.23
	Memory: Real Memory	GB	2.076 of 2.467 GB = 84.13%
	Virtual Memory: Swap Space	GB	0 of 2 GB = 0.00%
▲	Disk: /	MB	487.4 of 988.2 MB = 49.32%

The Events Browser

Network Discovery logs network and access events in your network. It can display up to 1,000 events at a time.

A network event occurs when:

- a device attribute changes alarm state (from OK to major, minor to major, major to minor, major to critical, and so on)
- a device or port is physically added, deleted, or moved
- the user changes a device or port property through Network Discovery (with the Device Properties or Port Properties dialog)

An access event occurs when:

- users access (or attempt to access), or logout of the Peregrine appliance
- an admin or IT manager user writes to a device MIB

Note: Only admin accounts can view access events.

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.

Important: The Events Browser shows events for the past 45 days or up to a maximum of 500,000 events (whichever is less).

Opening the Events Browser

To open the Events Browser:

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

OR

▶ On the Home page click the **Events Browser** link.

OR

- From a map window, Health Panel, Alarms Viewer, Service Analyzer, or MIB Browser, click **Tools** > **Events Browser**.

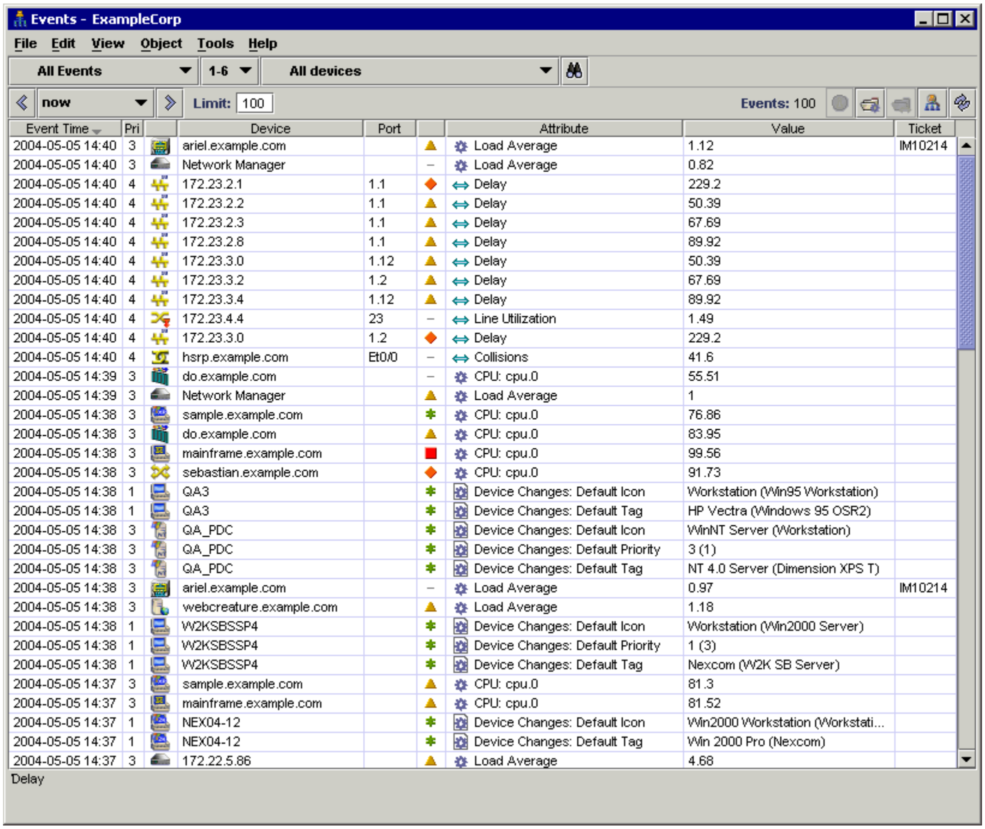
  OR

- From a Device Manager or Port Manager (button on Toolbar).

Network Events

All users can see the network events on the Events Browser. Figure 6-2 shows an example of what you will see if you selected All Events from the events pull-down list. If you select one type of event from the list, the display will change, and you will see only that event, and columns relating to that event-type.

Figure 6-2: Events Browser showing network events



All Events ▾ 1-6 ▾ All devices ▾

now ▾ Limit: 100 Events: 100

Event Time	Pri	Device	Port		Attribute	Value	Ticket
2004-05-05 14:40	3	ariel.example.com		▲	Load Average	1.12	IM10214
2004-05-05 14:40	3	Network Manager		–	Load Average	0.82	
2004-05-05 14:40	4	172.23.2.1	1.1	◆	Delay	229.2	
2004-05-05 14:40	4	172.23.2.2	1.1	▲	Delay	50.39	
2004-05-05 14:40	4	172.23.2.3	1.1	▲	Delay	67.69	
2004-05-05 14:40	4	172.23.2.8	1.1	▲	Delay	89.92	
2004-05-05 14:40	4	172.23.3.0	1.12	▲	Delay	50.39	
2004-05-05 14:40	4	172.23.3.2	1.2	▲	Delay	67.69	
2004-05-05 14:40	4	172.23.3.4	1.12	▲	Delay	89.92	
2004-05-05 14:40	4	172.23.4.4	23	–	Line Utilization	1.49	
2004-05-05 14:40	4	172.23.3.0	1.2	◆	Delay	229.2	
2004-05-05 14:40	4	hsrp.example.com	Et0/0	–	Collisions	41.6	
2004-05-05 14:39	3	do.example.com		–	CPU: cpu.0	55.51	
2004-05-05 14:39	3	Network Manager		▲	Load Average	1	
2004-05-05 14:38	3	sample.example.com		✱	CPU: cpu.0	76.86	
2004-05-05 14:38	3	do.example.com		▲	CPU: cpu.0	83.95	
2004-05-05 14:38	3	mainframe.example.com		■	CPU: cpu.0	99.56	
2004-05-05 14:38	3	sebastian.example.com		◆	CPU: cpu.0	91.73	
2004-05-05 14:38	1	QA3		✱	Device Changes: Default Icon	Workstation (Win95 Workstation)	
2004-05-05 14:38	1	QA3		✱	Device Changes: Default Tag	HP Vectra (Windows 95 OSR2)	
2004-05-05 14:38	3	QA_PDC		✱	Device Changes: Default Icon	WinNT Server (Workstation)	
2004-05-05 14:38	3	QA_PDC		✱	Device Changes: Default Priority	3 (1)	
2004-05-05 14:38	3	QA_PDC		✱	Device Changes: Default Tag	NT 4.0 Server (Dimension XPS T)	
2004-05-05 14:38	3	ariel.example.com		–	Load Average	0.97	IM10214
2004-05-05 14:38	3	webcreature.example.com		▲	Load Average	1.18	
2004-05-05 14:38	1	W2KSBSSP4		✱	Device Changes: Default Icon	Workstation (Win2000 Server)	
2004-05-05 14:38	1	W2KSBSSP4		✱	Device Changes: Default Priority	1 (3)	
2004-05-05 14:38	1	W2KSBSSP4		✱	Device Changes: Default Tag	Nexcom (W2K SB Server)	
2004-05-05 14:37	3	sample.example.com		▲	CPU: cpu.0	81.3	
2004-05-05 14:37	3	mainframe.example.com		▲	CPU: cpu.0	81.52	
2004-05-05 14:37	1	NEX04-12		✱	Device Changes: Default Icon	Win2000 Workstation (Workstati...	
2004-05-05 14:37	1	NEX04-12		✱	Device Changes: Default Tag	Win 2000 Pro (Nexcom)	
2004-05-05 14:37	3	172.22.5.86		▲	Load Average	4.68	

Delay

Each row in the Events Browser window contains the following columns.

Table 6-1: Data in Events Browser table

Data	Explanation
Time	The time the event was generated.
Device Priority	—
Device type	small device icon
Device	device title[a]
Port	port number
State	alarm icon
Attribute	For more information on the attributes, see the *Reference Manual*.
Value	For more information on the attributes, see the *Reference Manual*.
Ticket	ServiceCenter ticket number

[a] If no device title can be determined, the Events Browser displays “[Unknown]”. This depends on the Device Title Preferences as set in **Administration** > **System preferences** > **Display preferences**.

“Broadcast In” and “Broadcast out” alarms are not logged, due to the potentially very high number of events. “Source of Broadcast” alarms are logged.

Access Events

Only admin accounts can view access events on the Events Browser. You can select any of the these event types to view:

- Appliance Access
- SNMP Write by MIB OID
- SNMP Write by Attribute

Similar to the network events list, the columns will change depending on the type of event you choose to display.

Appliance Access events show the following data:

Table 6-2: Appliance Access events data

Data	Explanation
Event time	the time of the access event
Account name	the user accessing Network Discovery
From IP	the IP address from which the user accessed Network Discovery
Access point	the part of Network Discovery accessed by the user: ■ MIB Browser – the user has accessed the MIB Browser. ■ Network Map – the user has accessed the Network Map. ■ HTTP – the user has successfully logged into Network Discovery. ■ Telnet Proxy – the first time this account has logged into a remote appliance through the aggregator. ■ HTTP Proxy – the first time this account has logged into a remote appliance through the aggregator. ■ MIB Browser Proxy – the first time this account has opened a MIB Browser session on a remote appliance through the aggregator. ■ Applet Server – the user has accessed the Network Map, Health Panel, or another applet in the Network Discovery user interface. ■ Network Map Proxy – the first time this account has opened a Network Map session on a remote appliance through the aggregator. ■ Share – the user has accessed the shared directory on the Peregrine appliance.
Access status	whether or not the user was able to access Network Discovery: ■ Connect – the user has connected to Network Discovery, and disconnected without attempting to login. ■ Login OK – the user has successfully logged in to Network Discovery. ■ Login fail – the user has attempted to login, and did not have the correct password. ■ Logout – the user has logged out of Network Discovery.[a] ■ Login disabled – the user has tried to login with a failed password too many times (limit has been set in **Administration** > **Account administration** > **Appliance passwords**) ■ Login no permission – this account has been denied permission to access Network Discovery.

[a] Logout for HTTP and HTTP proxy has a timeout of 5 minutes from your last HTTP request.

SNMP Write events show the following data:

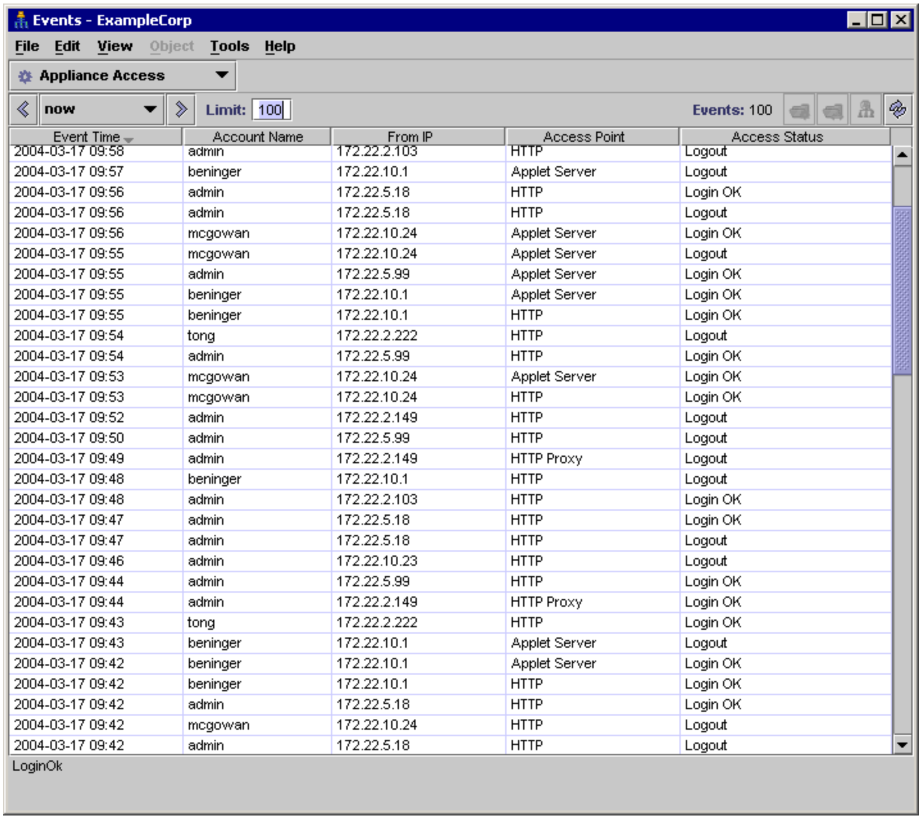
Table 6-3: SNMP Write events

Data	Explanation
Event time	the time of the access event
Account name	the user accessing Network Discovery
From IP	the IP address from which the user accessed the device
To IP	the device that had its MIB changed
MIB OID	the MIB OID changed by the user (for "Write by MIB OID" only)
Attribute	either Administrative Status or Bridge Aging Interval, these being the only attributes a user can change through the MIB (for "Write by Attribute" only)
Write Community String	the community string used to access the MIB
Value	the new "changed" value of the OID
Access Status	whether or not the user was able to write to the MIB: ■ Write OK ■ Fail (any of the following messages may appear): invalid response, too big, no such name, bad value, read only, gen err, no access, wrong type, wrong length, wrong encoding, wrong value, no creation, inconsistent value, resource unavailable, commit failed, undo failed, authorization error, not writable.

To view access events on the Events Browser

▶ Click **View** > **Show Access Events.**

Figure 6-3: Events Browser showing access events



Appliance Access

now

Limit: 100

Events: 100

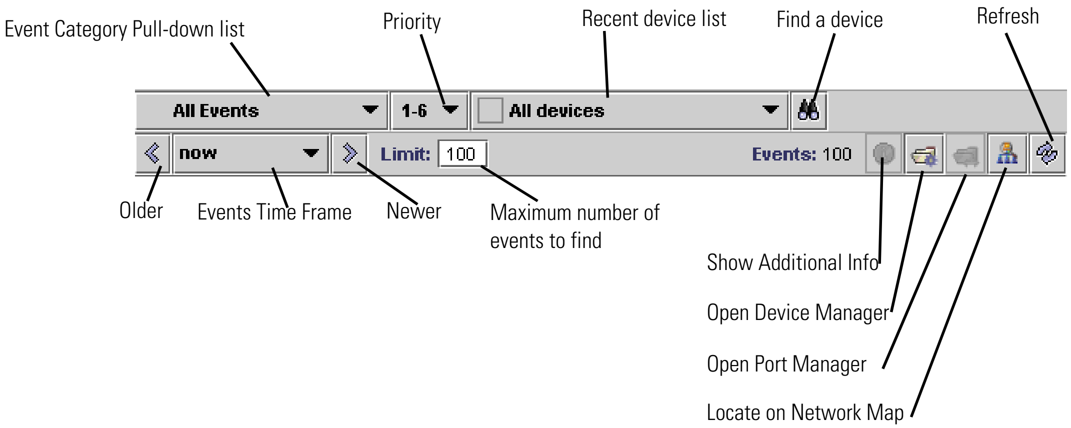
Event Time	Account Name	From IP	Access Point	Access Status
2004-03-17 09:58	admin	172.22.2.103	HTTP	Logout
2004-03-17 09:57	beninger	172.22.10.1	Applet Server	Logout
2004-03-17 09:56	admin	172.22.5.18	HTTP	Login OK
2004-03-17 09:56	admin	172.22.5.18	HTTP	Logout
2004-03-17 09:56	mcgowan	172.22.10.24	Applet Server	Login OK
2004-03-17 09:55	mcgowan	172.22.10.24	Applet Server	Logout
2004-03-17 09:55	admin	172.22.5.99	Applet Server	Login OK
2004-03-17 09:55	beninger	172.22.10.1	Applet Server	Login OK
2004-03-17 09:55	beninger	172.22.10.1	HTTP	Login OK
2004-03-17 09:54	tong	172.22.2.222	HTTP	Logout
2004-03-17 09:54	admin	172.22.5.99	HTTP	Login OK
2004-03-17 09:53	mcgowan	172.22.10.24	Applet Server	Login OK
2004-03-17 09:53	mcgowan	172.22.10.24	HTTP	Login OK
2004-03-17 09:52	admin	172.22.2.149	HTTP	Logout
2004-03-17 09:50	admin	172.22.5.99	HTTP	Logout
2004-03-17 09:49	admin	172.22.2.149	HTTP Proxy	Logout
2004-03-17 09:48	beninger	172.22.10.1	HTTP	Logout
2004-03-17 09:48	admin	172.22.2.103	HTTP	Login OK
2004-03-17 09:47	admin	172.22.5.18	HTTP	Login OK
2004-03-17 09:47	admin	172.22.5.18	HTTP	Logout
2004-03-17 09:46	admin	172.22.10.23	HTTP	Logout
2004-03-17 09:44	admin	172.22.5.99	HTTP	Login OK
2004-03-17 09:44	admin	172.22.2.149	HTTP Proxy	Login OK
2004-03-17 09:43	tong	172.22.2.222	HTTP	Login OK
2004-03-17 09:43	beninger	172.22.10.1	Applet Server	Logout
2004-03-17 09:42	beninger	172.22.10.1	Applet Server	Login OK
2004-03-17 09:42	beninger	172.22.10.1	HTTP	Login OK
2004-03-17 09:42	admin	172.22.5.18	HTTP	Login OK
2004-03-17 09:42	mcgowan	172.22.10.24	HTTP	Logout
2004-03-17 09:42	admin	172.22.5.18	HTTP	Logout

LoginOk

Toolbar

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 6-4: Events Browser toolbar



Event Category Pull-down List

Selects the category of events for display so that you can focus on a specific event type.

Priority

Selects the priority of devices you want to see.

Device pull-down list

This is a list of recently seen devices. You can toggle between these devices to see the events on each device.

A device will appear on this list by being selected on the map, the Alarms Viewer, or the Events Browser.

Find Device

By clicking the “Find” button, you can find a single device and see only the events on that device.

Refresh

Refreshes the events shown.

Limits Does not re-read the data in the panel from the network. Re-reads the data only from the Network Discovery database.

Older

Updates the window with earlier events, relative to currently displayed events.

Limits 45 days ago (or 500,000 events, whichever is less)

Events Time Frame

This pull-down list lets you select older events from a particular time.

Limits Now | 1 hour ago | 2 hours ago | 4 hours ago | 8 hours ago | 16 hours ago | 1 day ago | 2 days ago | 4 days ago | 1 week ago | 2 weeks ago | 4 weeks ago

Default Now

Newer

Updates the window with later events, relative to currently displayed events.

Limits current time

Limit

Set the maximum number of events per window.

Limits 1–1000

Default 25

Events

Shows the number of events listed in the window.

Open Device Manager

Clicking this button will open the Device Manager for the selected device.

Open Port Manager

Clicking this button will open the Port Manager for the selected port.

Locate Device on Network Map

Clicking this button will locate the device on the Network Map.

The Service Analyzer

The Network Discovery Service Analyzer allows you to analyze the network path between 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.

Choosing your Path

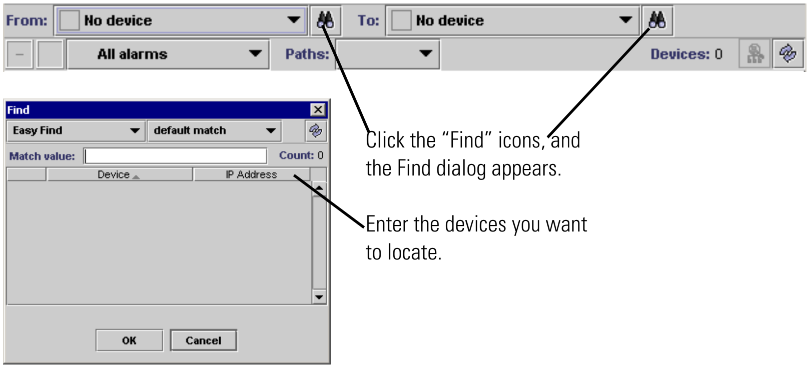
The toolbar contains two search boxes: **From** and **To**. Each box searches for a device based on its name, title, or address. This Find window works exactly the same way as the global Find feature. For more information, see *Find* on page 94.

To use the Service Analyzer

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

Note: Also, you can open the Service Analyzer from the Device Manager. That device will be the first device in the Service Analyzer query.

Figure 6-5: Service Analyzer toolbar



Click the “Find” icons, and the Find dialog appears.

Enter the devices you want to locate.

2. Click the first Find icon.
3. Enter the IP address of the first device you want to find, and press ENTER.
4. Select a device from the Find dialog and click **OK**.
5. Repeat step 2 to step 4 for the second Find icon.

Note: It is important to fill in the device on the left first. Changing the device on the left side will automatically clear the device on the right side.

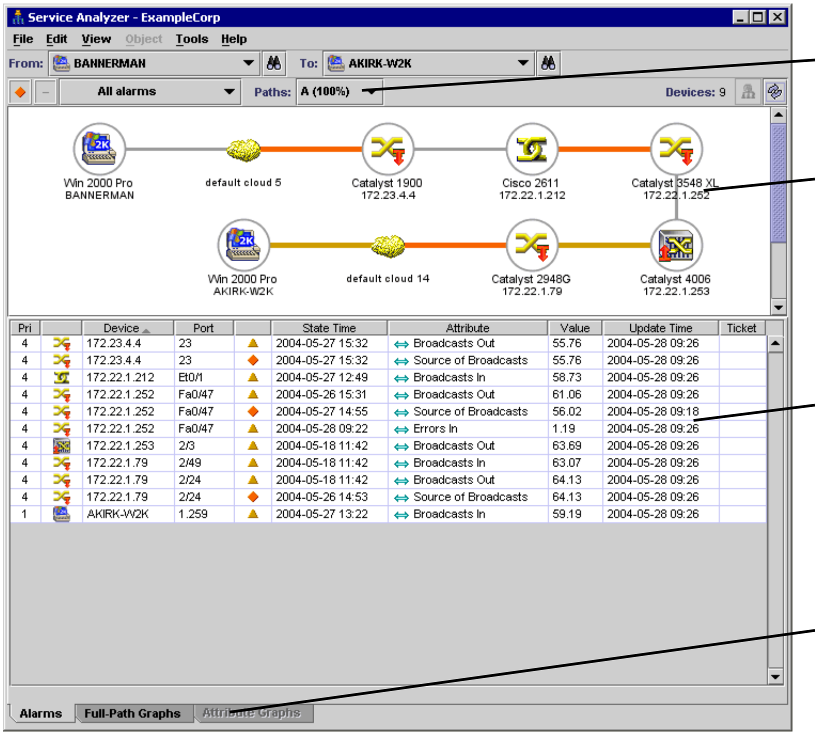
Alarms Tab

By default, you will see the Alarms Tab first. You will see the path diagram, a summary graph for the path displayed, and a list of alarms for the devices in that path.

There are two areas on the Alarms Tab:

- Path Diagram
- Alarm List

Figure 6-6: Service Analyzer Window (Alarms Tab)



Pri		Device	Port		State Time	Attribute	Value	Update Time	Ticket
4		172.23.4.4	23	▲	2004-05-27 15:32	⇔ Broadcasts Out	55.76	2004-05-28 09:26	
4		172.23.4.4	23	◆	2004-05-27 15:32	⇔ Source of Broadcasts	55.76	2004-05-28 09:26	
4		172.22.1.212	Et0/1	▲	2004-05-27 12:49	⇔ Broadcasts In	58.73	2004-05-28 09:26	
4		172.22.1.252	Fa0/47	▲	2004-05-26 15:31	⇔ Broadcasts Out	61.06	2004-05-28 09:26	
4		172.22.1.252	Fa0/47	◆	2004-05-27 14:55	⇔ Source of Broadcasts	56.02	2004-05-28 09:18	
4		172.22.1.252	Fa0/47	▲	2004-05-28 09:22	⇔ Errors In	1.19	2004-05-28 09:26	
4		172.22.1.253	2/3	▲	2004-05-18 11:42	⇔ Broadcasts Out	63.69	2004-05-28 09:26	
4		172.22.1.79	2/49	▲	2004-05-18 11:42	⇔ Broadcasts In	63.07	2004-05-28 09:26	
4		172.22.1.79	2/24	▲	2004-05-18 11:42	⇔ Broadcasts Out	64.13	2004-05-28 09:26	
4		172.22.1.79	2/24	◆	2004-05-26 14:53	⇔ Source of Broadcasts	64.13	2004-05-28 09:26	
1		AKIRK-W2K	1.259	▲	2004-05-27 13:22	⇔ Broadcasts In	59.19	2004-05-28 09:26	

If more than one path is used, you can see the different paths here.

Path Diagram

Alarm List

Tab selector

Path Diagram

The Path diagram shows the path between the two selected devices.

You will notice that the path diagram has a similar look to the Network Map. Devices and lines will appear as they would on a map, with colored circles and lines representing different alarm states. The path diagram presents only devices and lines. Packages are not shown.

In the “Paths” pull-down list, multiple views are available to display the data for different paths between the two devices.

Note: If there is only a single path, it will be the only choice. The percentage indicates how frequently a path was taken. If the sum of the percentages is less than 100, it indicates a device in the path was off or broken for some time over the preceding 48 hours.

Note: The Alarms panel will only display attribute alarms. If there are report alarms on a device or port, you will see them listed in the Alarms Viewer, in the Device Manager, or on the Network Map. (For a full list of report alarms and attribute alarms, see **Help** > **Classifications** > **Alarms.**)

Note: You can select alarms from the pull-down list if you want to see only one alarm-type.

Alarm list

If any problems are detected on the path, they are summarized in a table underneath the graphs.

Table 6-4: Problems detected on the path

Column	Notes	Example
Priority	—	—
Device Type	—	—
Device	double-click to open the Device Manager	rbuffin.example.com
Port	—	—
State	—	—
State Time	—	—
Attribute	attribute name	Errors In
Value	For more information on the attributes, see the *Reference Manual.*	2.07 frames/sec.
Update Time	the time it was last polled	—
Ticket	ServiceCenter ticket number	—

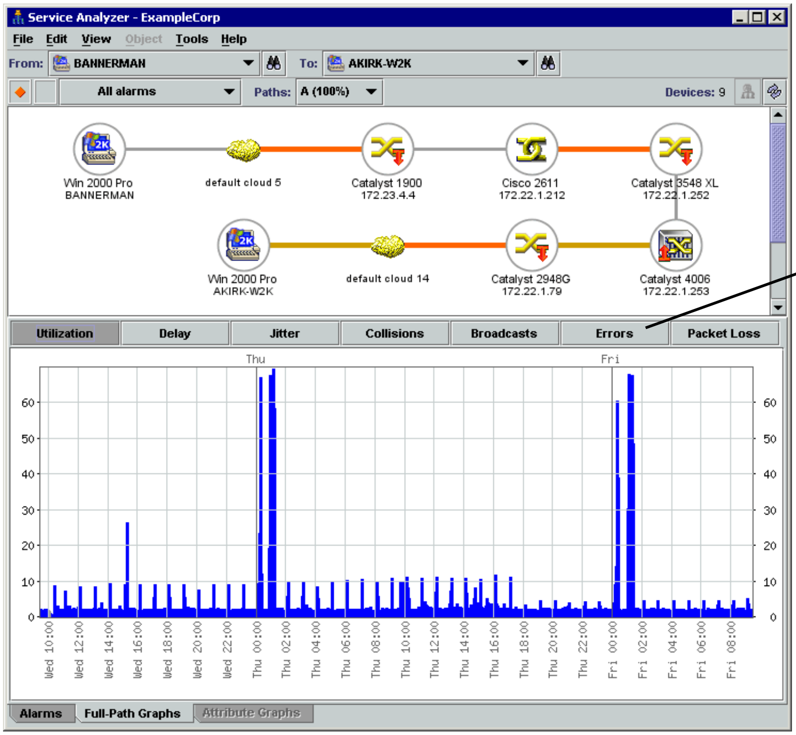
Full-Path Graphs

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

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

You can click any of the buttons to view the related alarm category.

Figure 6-7: Full-Path Graphs tab



Service Analyzer - ExampleCorp

From: BANNERMAN

To: AKIRK-W2K

All alarms

Paths: A (100%)

Devices: 9

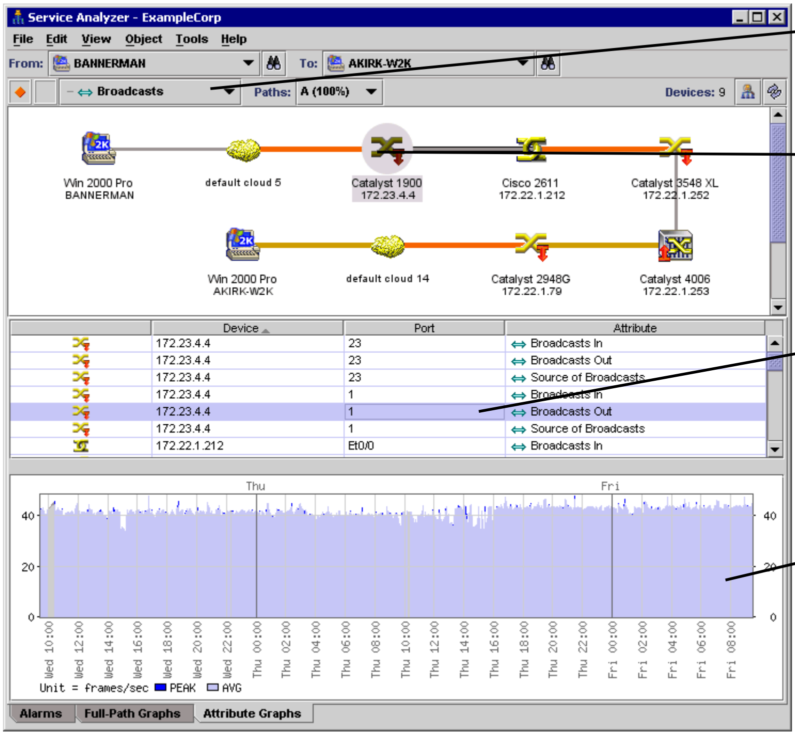
Select one of these buttons to display the graphs

All graphs display traffic levels for the last 48 hours across the entire path.

Attribute Graphs Tab

You can enable the Graphs panel by selecting an alarm category from the pull-down list (i.e., you cannot see the Graphs panel if "All Alarms" is selected).

Figure 6-8: Service Analyzer Window (Graphs Tab)



Service Analyzer - ExampleCorp

From: BANNERMAN

To: AKIRK-W2K

Broadcasts

Paths: A (100%)

Devices: 9

	Device	Port	Attribute
	172.23.4.4	23	Broadcasts In
	172.23.4.4	23	Broadcasts Out
	172.23.4.4	23	Source of Broadcasts
	172.23.4.4	1	Broadcasts In
	172.23.4.4	1	Broadcasts Out
	172.23.4.4	1	Source of Broadcasts
	172.22.1.212	Et0/0	Broadcasts In

1 - Select an alarm category

2 - Select a device in the path

3 - The device is also selected in the device list.

4 - The related graph is displayed.

Individual Device/Port Graph List

This list displays all the devices in the selected path, and shows data for the selected alarm category. For example, as seen in Figure 6-5, you can see all the Broadcast information for the devices.

Graph Display Area

This area displays alarm graphs for the individual devices and ports in the path.

For example, you can select one device in the path (172.23.4.4) and select an alarm category (Broadcasts), and see that graph.

Find

The Find command lets you locate and examine any device on the network. There is also an Aggregate Find feature. For more information, see *The Aggregate Find* on page 209.

Finding devices

To use the Find tool

1 Open the Find tool:

a On the main Toolbar click the **Find** button.

OR

b On the Home page click **Find**.

OR

c From a map window, Health Panel, Alarms Viewer, Events Browser, or MIB Browser, click **Tools** > **Find** (or Ctrl-F).

2 By default, you can use the **Easy Find** feature. If you want to do a more advanced find, continue with the next step in this procedure.

3 In the first pull-down list, select the device data you want to find (for example, “asset tag”).

4 In the second pull-down list, select a match mode (for example, “containing”).

Note: There are different match modes available for different types of device data.

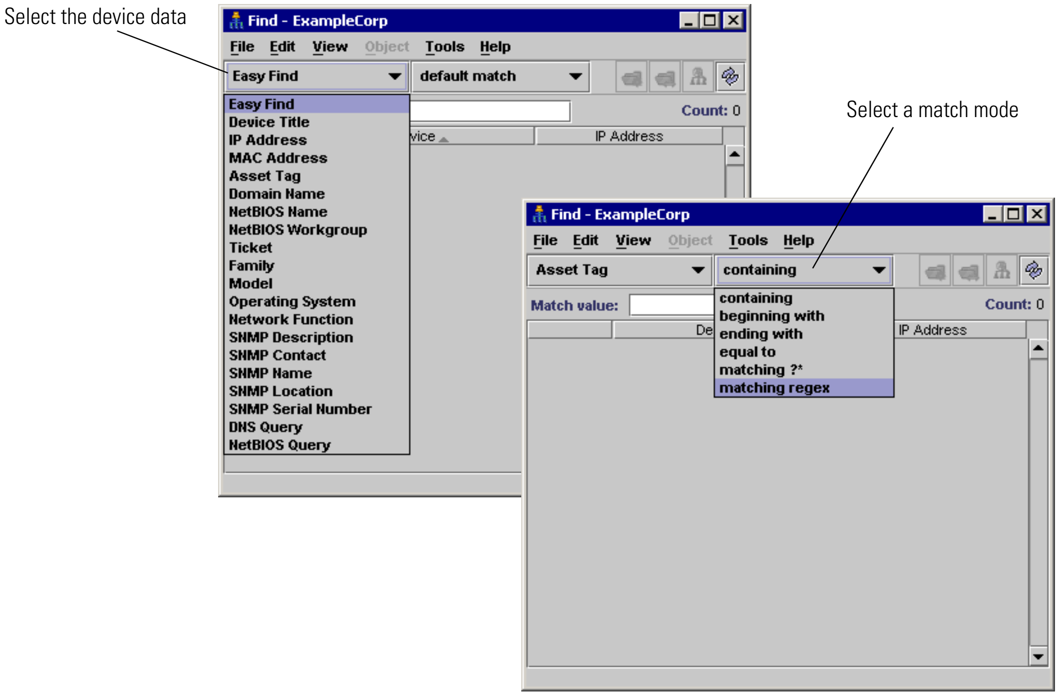
5 Enter a match value.

Note: To find multiple devices in the Network Discovery database, enter the first letter of a title or the first number of an address.

6 Press **Enter**.

Network Discovery searches for the device. The results of the search appear in table format, and you can select the device you want to open.

Figure 6-9: The Find Window



Easy Find

When you enter text into the Find box, Network Discovery searches the network in the following order (if there is no result at one stage, Network Discovery will try the next):

Example: Once an IP address has been found, Network Discovery does not search domain names and device titles.

Find Method	Explanation
“localhost” or “nmc”	These are two shortcuts for finding the Peregrine appliance.
MAC address	Network Discovery will try to search based on the known MAC address. **Note:** To find a specific device, you must enter its complete MAC address.
IP address	Network Discovery will try to search based on the known IP address. **Note:** To find a specific device, you must enter its complete IP address.
Domain Name	Network Discovery searches based on the DNS suffix as configured in **Administration** > **Appliance management** > **Domain name servers.**
Device Title	Network Discovery will then search the network based on your device title preferences from **Administration** > **System preferences** > **Display preferences** > **Device title preference.**
Asset Tag	Even if Asset Tag is not listed in your Device title preference, Network Discovery will search for it next.
NetBIOS Name	Even if NetBIOS name is not listed in your Device title preference, Network Discovery will search for it next.

Important: Only the options that have been selected in **Administration** > **System preferences** > **Display preferences** affect the title search. For example, if you ask Network Discovery to search for devices with the Last Name “Tremblay”, but the Last Name option has not been selected, the search will fail even if the device is on the Network Map.

Important: All multiple results are based on the device title. Example: If you enter “192.168.2.”, you will not find all devices 192.168.2.0–192.168.2.255. You will only find devices with “192.168.2.” in the title. If the device with IP address 198.168.2.55 takes it title from its domain name, that device will not be found.

Advanced Find

Note: Searches are not case-sensitive.

Match Modes	Notes
containing	—
beginning with	—
ending with	—
equal to	—
matching ?*	Wildcard characters: ■ “?” can represent any single character. For example, “gr?y” finds “gray” and “grey.” ■ “*” can find multiple characters. For example, “E*t” finds “Ethernet.”
matching regex	Matching a regular expression.
matching address*	This works only for IP address and MAC address searches. You must enter an entire IP or MAC address in these formats: ■ IP - 123.123.123.123 ■ MAC - 12:12:12:12:12:12 **Note:** You can substitute a * for an octet in an IP address octet or a segment of a MAC address. For example: “123.*.123.123” or 12:12:*:12:12:12 **Note:** For MAC addresses, you can compress the zeros in each segment. For example, you can enter “5” instead of “05” for a segment. **Note:** If an IP or MAC address is associated with a port, you will see a port listed in your Find results.
name prefix	—
name equal to	—

Note: If you have configured Network Discovery to work with ServiceCenter, you will be able to Find ticket numbers.

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 *Setup Guide*.

To learn about the options available in the administration pages, read the help associated with each page.

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 Scanned Machine Reports).

For more information on reports, see the *Reference Manual*.

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
- What devices are active in your Network Map
- What devices are deactivated from your Network Map
- What devices are hidden from your Network Map
- What forced connections exist on your Network Map

CHAPTER 7

Customizing Your View of the Network Map

There are several ways you can change the look and feel of your Network Map. Your account-type determines the preferences and properties you are allowed to change.

All accounts can change preferences such as line style, background color, background image, and scale.

Administrator or IT Manager users have the option of changing Device Properties such as device icon, device title, and so on (from the Network Map, click **Object** > **Device Properties**). These properties will affect all accounts.

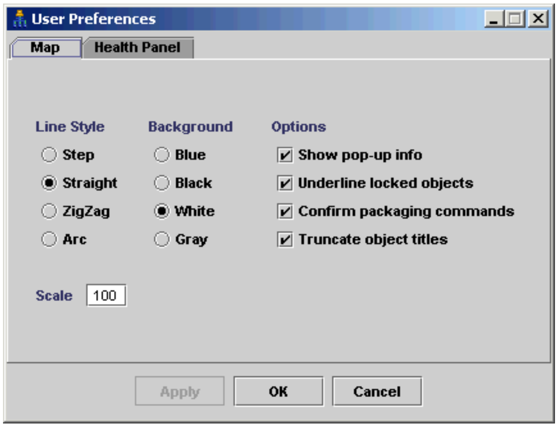
Topics in this chapter include:

Changing Map Preferences

Customizing how you see the map

You can change the look of your Network Map in several ways.

Figure 7-1: User Preferences dialog



Line Style
○ Step
● Straight
○ ZigZag
○ Arc

Background
○ Blue
○ Black
● White
○ Gray

Options
☑ Show pop-up info
☑ Underline locked objects
☑ Confirm packaging commands
☑ Truncate object titles

Scale 100

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
- Arc

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:

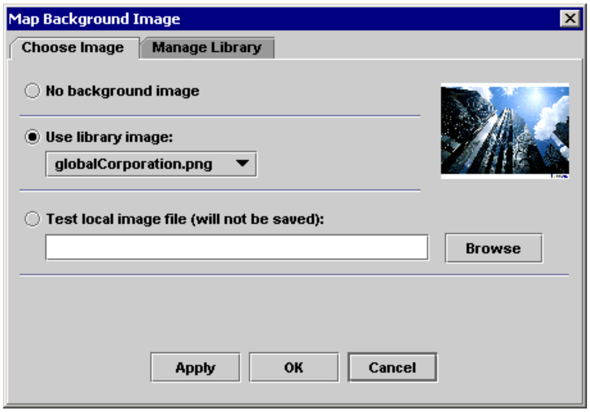
- Blue
- Black
- White
- Gray

3 Click **OK**.

Changing the map background image

You can add images to your Network Map background (main map and packages).

There is a library of images you can select, all of which are available to all users. An Administrator or IT Manager account can add more pictures to the library (see *Managing your background image library* on page 115).



Map Background Image

Choose Image | Manage Library

○ No background image

● Use library image: globalCorporation.png

○ Test local image file (will not be saved):

To test an image file from your computer

1 Click **Configure** > **Background Image**.

The Map Background Image dialog appears.

2 Select **Test Local Image File** and browse to find the file you want.

3 Click **Apply**.

Note: This background will not be saved as part of your map configuration. Only files in the image library can be saved.

To select an image file from the library

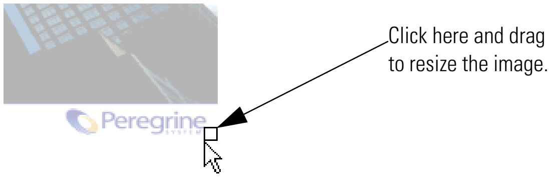
1 Click **Configure** > **Background Image.**

The Map Background Image dialog appears.

2 Select an image from the image library pull-down list.

3 Click **Apply.**

The image will appear as the background of your map window. By default, the image will cover the entire map window. You can alter the size of the image by clicking and dragging the image from its bottom-right corner.



Click here and drag to resize the image.

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 Click **Edit** > **User Preferences** > **Map.**

2 Enter a value between 1 and 200 in the “Scale” text box.

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%.)

On the Network Map Status bar, you can see the scale slider. You can click this and change the scale to from as small as 1% up to 200%. You can also type in a number into the text box, and hit Enter on your keyboard to initiate the change.

There are other options, described below.

To change the scale of this window

▶ Click **View** > **Zoom In**.

OR

▶ Click **View** > **Zoom Out**.

OR

▶ Click **View** > **Scale To Fit Width**.

OR

▶ Click **View** > **Scale To Fit Height**.

OR

▶ Click **View** > **Scale at 100%**.

Note: These commands are also available if you right-click on the scale slider.

Changing other viewing preferences

Show pop-up info

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

To show pop-up info

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

Underline locked objects

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

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

To underline locked objects

1. Click **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
- Unpackage
- Pack
- Unpack
- Unpack All

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

Truncate Object Titles

This preference lets you decide if you want to truncate object titles on your map. Sometimes, the object titles are very long, and Network Discovery will automatically truncate them to save space on the map. If you would rather have the full object name appear on the map, you can change it.

To truncate object titles

1. Click **Edit** > **User Preferences** > **Map**.
2. Click the box beside **Truncate object titles.**

Open Health Panel with Network Map

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

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

To open the Health Panel with the Network Map

1. Click **Edit** > **User Preferences** > **Health Panel.**
2. Click the box beside **Open Health Panel with Network Map**.

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 **Top of Network.**

   A confirmation message appears.
3. Click **Top of Network.**

   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.

   The **Top of Network** command should have a checkmark with it, indicating that you have previously chosen this object to be at the top of the window.
2. From the **Object** menu, click **Top of Network.**

   A confirmation message appears.
3. Click **Top of Network.**

The window is redrawn with the default icon at the top, as chosen by Network Discovery.

Layout

The Layout command reorganizes the layout of the active map window, then redraws the window. Use it to tidy a map with confusing layout and crisscrossing connections.

To clean up a map window

- Click **Configure** > **Layout.**

This command will destroy any custom layout, but will not affect any of the packaging.

Promoting objects

The Promote command moves the selected objects to the window one level above the current window (in terms of hierarchy, not screen space).

To promote an object

- Click **Configure** > **Promote.**

This command locks all selected objects (unless they are promoted into the Main Map).

Note: When the last object is promoted out of the package, the package is destroyed.

Reverting your map changes

If you are making changes to your map layout, and decide not to save your changes, you can **Revert** your map. This way, the autosave function will not save your changes.

Note: This feature works for changes to your map layout and packaging. Changes to the device properties (device tag, title, icon, or priority) or port properties cannot be reverted.

To revert your map to the version you last saved

1. Click **File** > **Revert.**

A warning dialog appears.

2 Click **OK.**

Customizing for IT Manager and Administrator accounts

This section is for IT Manager and Administrator accounts. IT Manager and Administrator accounts can also perform all of the procedures described in the section, *Changing Map Preferences* on page 102.

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

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

Table 7-1: Changing objects—Administrator and IT Manager accounts

To change	Do this	Affects other accounts and maps	Also affects
icon—devices	see *Changing Device Properties* on page 110	✓	■ thresholds (all accounts) ■ whether event filters are applied (all accounts) ■ reports
icon—packages	see *To change the icon and title of your package* on page 121	—	—
tag	*Changing Device Properties* on page 110	—	—
derived title (devices)	see **Administration** > **System preferences** > **Display preferences**	✓	—
title	see *Changing Device Properties* on page 110	✓	—
priority (devices)	see *Changing Device Properties* on page 110	✓	whether event filters are applied (all accounts)
to top object	see *Placing an object at the top of the map window* on page 107	—	—

Changing Device Properties

If you have an Administrator or IT Manager account, you can change the following in the Device Properties dialog (**Object** > **Device Properties**):

- Device Icon
- Device Tag
- Device Title
- Device Priority

Warning: If you change a device icon or priority, it will affect your event filters. See *Setting up Event Filters* on page 147.

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

Changing a device icon can change how it is packaged. Certain icons are packaged automatically. For example, when you change an end node icon to an icon that is not an end node, the device may be automatically unpacked. If you change a device icon to an end node icon, that device can be automatically packaged with the end nodes. See **Administration** > **System preferences** > **Automatic packaging**.

You might increase the priority of a device that is important to you or a device that you will want to monitor more closely. Devices with priority 6 are the most important. The higher the number, the higher the priority and the greater the importance.

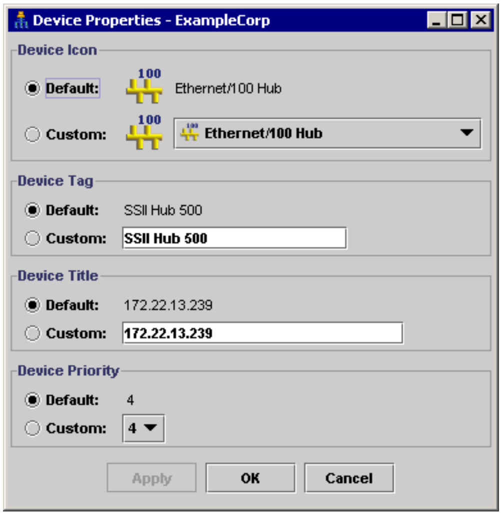
To change these Device Properties

1. With a device icon selected on the Network Map, click **Object** > **Device Properties**.

   The Device Properties dialog appears.
2. To change the device icon, select a new icon from the pull-down list.
3. To change the device tag, enter your own custom text.
4. To change the device title, enter your own custom text.
5. To change the device priority, select a new priority from the pull-down list.
6. Click **Apply**.
7. Click **OK**.

Note: As soon as you change the icon, Network Discovery will register a change event in the Events Browser.

Figure 7-2: Device Properties window



Device Properties - ExampleCorp

Device Icon

● Default: Ethernet/100 Hub

○ Custom: Ethernet/100 Hub

Device Tag

● Default: SSII Hub 500

○ Custom: SSII Hub 500

Device Title

● Default: 172.22.13.239

○ Custom: 172.22.13.239

Device Priority

● Default: 4

○ Custom: 4

To reset the Device Properties to the default settings

1 With a device icon selected on the Network Map, click **Object** > **Device Properties.**

The Device Properties dialog appears.

2 For the properties you wish to reset, select “Default.”

3 Click **Apply**.

4 Click **OK**.

Changing Alarm Thresholds

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

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

Copying alarm thresholds

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

To copy alarm thresholds

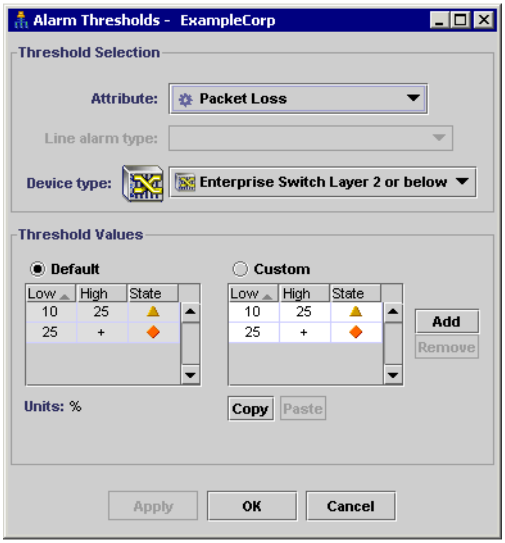
1. Select the custom alarm threshold setting you want to duplicate.
2. Click **Copy**.
3. Select an attribute from the pull-down list.
4. Select a line or device type from the pull-down list.
5. Click **Paste**.

   The alarm thresholds you selected in step 1 will now appear in the custom area of the Alarm Thresholds dialog for the newly selected attribute and device/line alarm type.
6. Click **Apply** to apply the changes.
7. Click **OK** to close the dialog.

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.

Figure 7-3: Alarm Thresholds (Device Types)



Alarm Thresholds - ExampleCorp

Threshold Selection

Attribute: Packet Loss

Line alarm type:

Device type: Enterprise Switch Layer 2 or below

Threshold Values

● Default

Low	High	State
10	25	▲
25	+	◆

Units: %

○ Custom

Low	High	State
10	25	▲
25	+	◆

To change the Device Alarm Thresholds

1 Select a device attribute from the pull-down list.

The **Device type** list is enabled.

2 Select a device type by clicking an icon from the pull-down list.

3 To change an alarm threshold, click a text box and enter a new number for the low or high value.

4 To create a new alarm threshold, click the **Add** button and a new row will appear.

5 To change the State of any alarm, click the box in the State column, and select the new state from the list that appears.

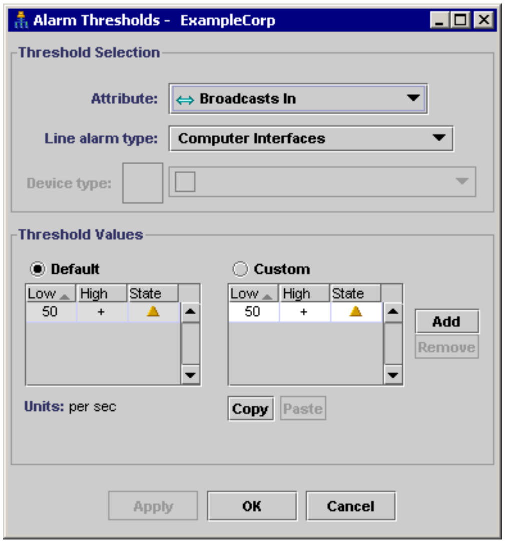
6 Click **Apply** or **OK**.

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

Line Alarm Types

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.

Figure 7-4: Alarm Thresholds (Line Types)



Alarm Thresholds - ExampleCorp

Threshold Selection

Attribute: Broadcasts In

Line alarm type: Computer Interfaces

Device type:

Threshold Values

● Default

Low	High	State
50	+	⚠

○ Custom

Low	High	State
50	+	⚠

Units: per sec

To change the Line Alarm Thresholds

1 Select a line attribute from the pull-down list.

The **Line alarm type** list is enabled.

2 Select a line alarm type by clicking an icon from the pull-down list.

3 To change an alarm threshold, click a text box and enter a new number for the low or high value.

4 To create a new alarm threshold, click the **Add** button and a new row will appear.

5 To change the State of any alarm, click the box in the State column, and select the new state from the list that appears.

6 Click **Apply** or **OK**.

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

Saving a map window as a graphic file

You can save any map window (the main map, or any package) as an image file (either jpg or png).

To save your map as an image file

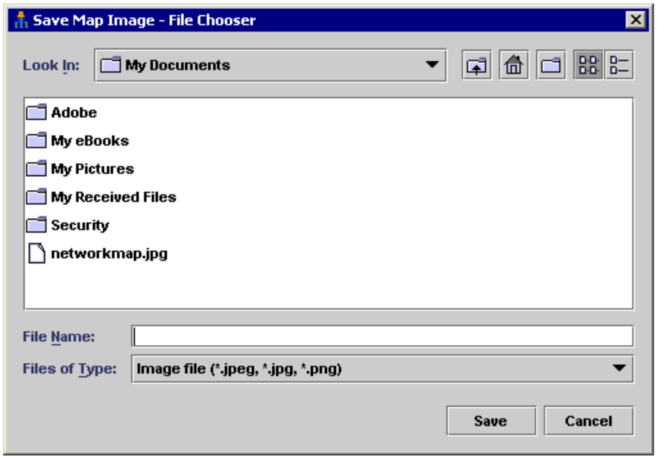
1 Click **File** > **Save Map Image.**

The File Chooser dialog appears.

2 Enter the name and location of the image file you want to save.

3 Select a file type.

4 Click **Save.**



Save Map Image - File Chooser

Look In: My Documents

Adobe
My eBooks
My Pictures
My Received Files
Security
networkmap.jpg

File Name:

Files of Type: Image file (*.jpeg, *.jpg, *.png)

Managing your background image library

An Administrator or IT Manager account can add and delete images from the Network Discovery image library. These images are available to every user, regardless of account type.

Important: If you add images that are larger than 250KB, you may notice the Network Map scrolling slowly.

Note: You will notice that the background images are dimmed slightly, so the image colors will not interfere with the map icons and lines. If you add your own images to the library, Network Discovery will automatically dim the images, so you need not alter your graphic files before adding them to the library.

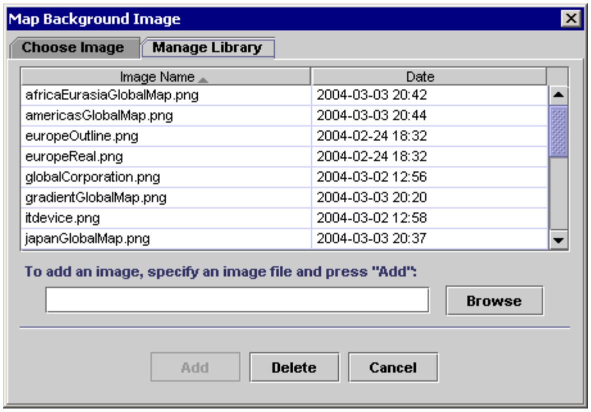


Image Name	Date
africaEurasiaGlobalMap.png	2004-03-03 20:42
americasGlobalMap.png	2004-03-03 20:44
europeOutline.png	2004-02-24 18:32
europeReal.png	2004-02-24 18:32
globalCorporation.png	2004-03-02 12:56
gradientGlobalMap.png	2004-03-03 20:20
itdevice.png	2004-03-02 12:58
japanGlobalMap.png	2004-03-03 20:37

To add an image, specify an image file and press "Add":

To add an image to the library

1. Click **Configure** > **Background Image.**

   The Map Background Image dialog appears.
2. Select the Manage Library panel.
3. Click **Browse** and search for your image file.
4. Click **Add.**

To delete an image from the library

1. Click **Configure** > **Background Image.**

   The Map Background Image dialog appears.
2. Select the Manage Library panel.
3. Select the file you want to delete.
4. Click **Delete.**

8 Packaging Your Network

CHAPTER

You can group objects into “packages” so that the map is more organized 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

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

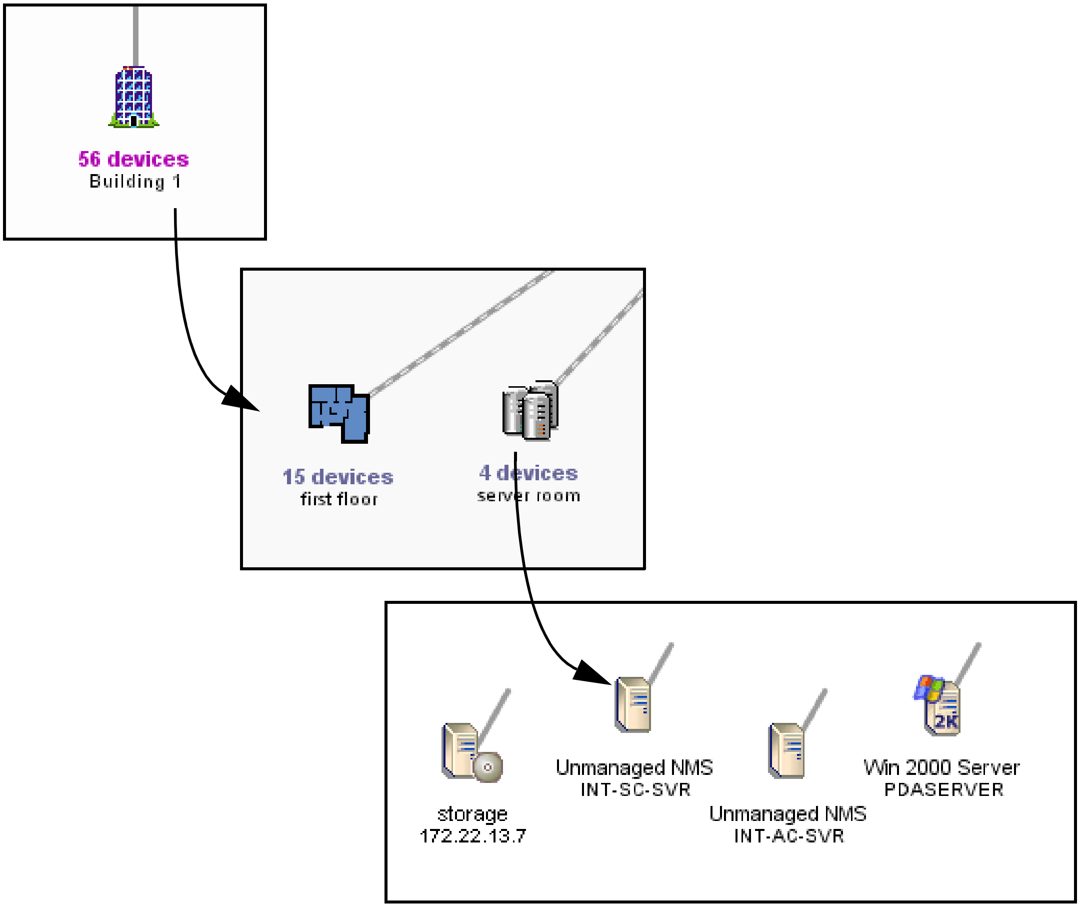
You can create packages to represent hierarchies, such as campuses, buildings, floors in buildings and so on. There are many package icons available to help you create the desired look and feel of the Network Map.

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 and the type you can create yourself.

One application of multi-object packaging is mapping the network at a physical location, such as a city. 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 the first floor and the server room. Drilling down further, you reach the devices for the “server room” within the end node package.

Figure 8-1: Location packages



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. Click **Configure** > **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 recreate all of the automatic 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. Click **Configure** > **Object** > **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 **Package**.

The object will absorb any dependent object that:

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

To change the icon and title of your package

1. With the package icon selected, click **Object** > **Package Properties**.
2. Select a custom package icon from the pull-down list.
3. Enter a custom title for the package.
4. Click **Apply** or **OK**.

You can also unpack your packages

To move the contents of the active package up one level

▶ From the package window, click **Configure** > **Promote All**.

This command causes the following:

- Only the current package window is destroyed. Packages within the current package are not destroyed.
- Unlocks all objects.
- Automatic packages that were within the window are repackaged.

Note: In the Main Map window, this command is replaced by **Unpack All**.

To unpack the entire Network Map, and destroy all packaging

▶ From the Main Map window, click **Configure** > **Unpack All**.

This command causes the following:

- All packages are destroyed.
- Unlocks all objects.
- Automatic packages are repackaged.

Note: In a package window, this command is replaced by **Promote All**.

To empty one package

▶ From any map window, with a package selected, click **Configure** > **Object** > **Unpackage**.

This command causes the following:

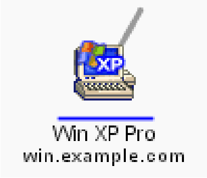
- Causes the selected package to be unpackaged, which also deletes the package
- Locks all objects within the package (unless they are unpackaged into the main map).

Note: Available to single packages only.

Locked objects

If you have manually packaged your map, 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 (**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 all automatic packages. To keep a device from being automatically packaged, you can lock the device by using the **Lock** command.

To use the Lock command

▶ Click **Configure** > **Object** > **Lock**.

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 automatically creates packages, based on the major connectivity devices in your network.

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.

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.

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

If you have an Administrator account, you can change whether or not each class of device is packaged.

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.

Also by default, whenever Network Discovery detects 10 or more network devices, it will automatically package those devices.

The defaults work well with most networks. You can change them to package the network in a particular way.

There are seven automatic package types available:

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

- Network Devices
- 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.

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

To create automatic packages of a particular type

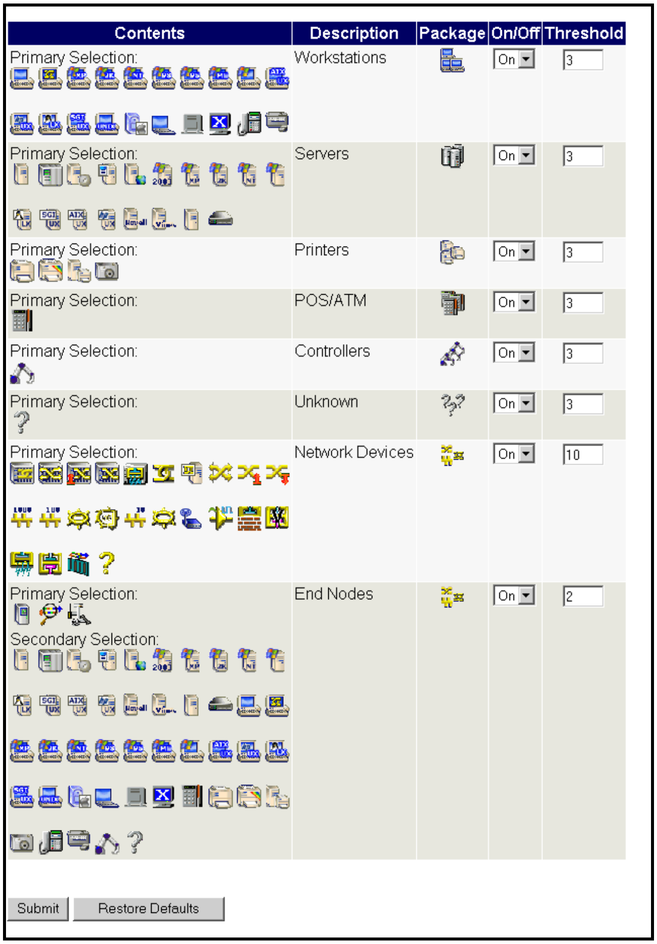
1. Click **Administration** > **System preferences** > **Automatic packaging.**
2. For the package types you want to create, turn the package type On.
3. Select a threshold for each type of package.

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

To restore the defaults

- ▶ Click **Restore Default.**

Figure 8-3: Automatic Packaging preferences



Contents	Description	Package	On/Off	Threshold
Primary Selection:	Workstations		On	3
Primary Selection:	Servers		On	3
Primary Selection:	Printers		On	3
Primary Selection:	POS/ATM		On	3
Primary Selection:	Controllers		On	3
Primary Selection:	Unknown		On	3
Primary Selection:	Network Devices		On	10
Primary Selection: Secondary Selection:	End Nodes		On	2

CHAPTER

9 Organizing Map Configuration Files

Network Discovery lets you save different map configuration files. Each of these map configurations contains your layout 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:

What is a Map Configuration?

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

Table 9-1: Default configuration files and accounts

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

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

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

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

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.

Note: If you have just installed and set up Network Discovery, you will notice that the Prime configuration does not exist. First, an Administrator account or IT Manager account must save a Prime configuration with the **Save As Prime** command (in a Network Map window, click **File** > **Save As Prime**).

Any user can open a copy of the Prime configuration in the Network Map by clicking **File** > **Open Copy of Prime**.

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, 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 bytes long (the number of characters depends on language encoding). You can use the following characters:

- A through Z (upper case)
- a through z (lower case)
- 0 though 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 Administrator 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, Network Map, and Health Panel stay open.

To open a saved map configuration

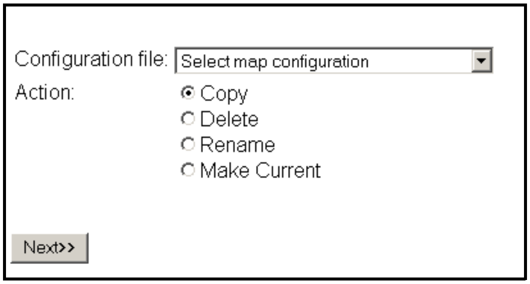
1. From the **File** menu, click **Open**.
2. Select the file name of the configuration you wish to use.
3. Click **OK**.

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



Configuration file: Select map configuration ▾

Action:
● Copy
○ Delete
○ Rename
○ Make Current

Next>>

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?” radio button. (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.

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

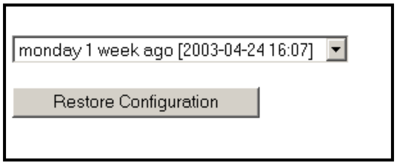
1 Click **Administration** > **Data management** > **Restore prime map configuration.**

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 9-2: Restore the Prime map configuration



monday 1 week ago [2003-04-24 16:07]

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

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 *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.

Configuring the SMTP server

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 SMTP server are in the *Setup Guide*.

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

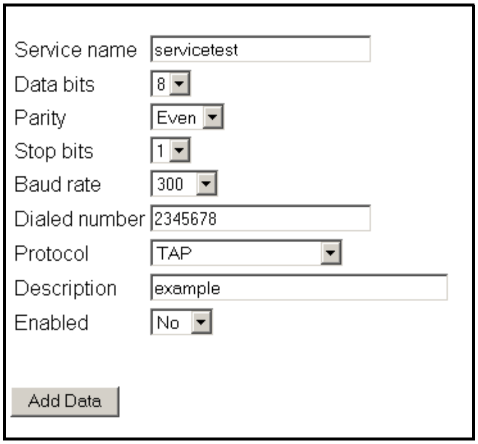
1. Click **Administration** > **Pager service provider configuration** > **Add a service provider.**
2. Enter a service name.

   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	servicetest
Data bits	8
Parity	Even
Stop bits	1
Baud rate	300
Dialed number	2345678
Protocol	TAP
Description	example
Enabled	No

Listing your service providers

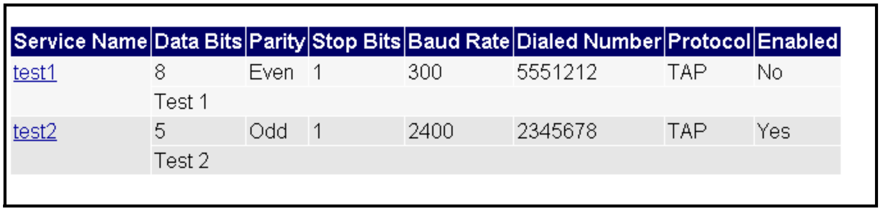
You may want to verify that you have correctly input the information for your pager service provider.

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
test1	8	Even	1	300	5551212	TAP	No
	Test 1						
test2	5	Odd	1	2400	2345678	TAP	Yes
	Test 2						

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.**

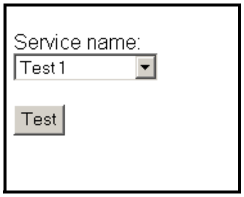
To test the selected service provider

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



Service name: Test 1

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.

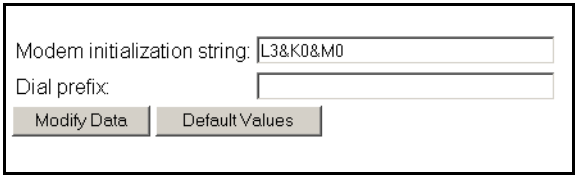
3 Click **Modify Data.**

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: L3&K0&M0

Dial prefix:

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.**

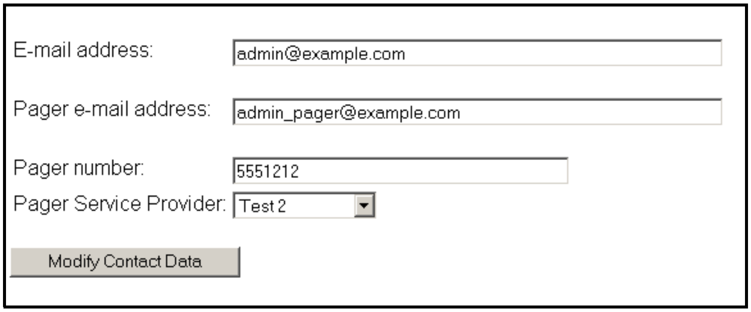
To enable paging through an e-mail gateway

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

To enable direct alphanumeric paging

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

Figure 10-5: Modify contact data



E-mail address: admin@example.com

Pager e-mail address: admin_pager@example.com

Pager number: 5551212

Pager Service Provider: Test 2

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 147.

Testing the pager address

This will send a test message to your pager, so that you can:

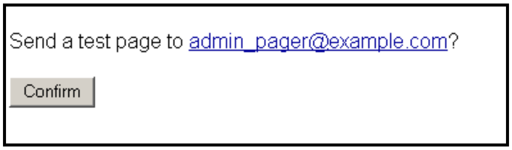
- test that you have entered your pager address correctly
- test that the Peregrine appliance has been configured to send messages to your pager

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



Send a test page to admin_pager@example.com?

Testing the pager number

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

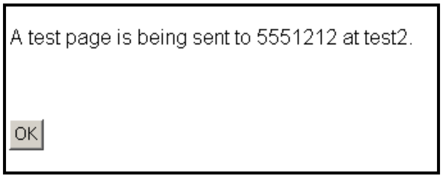
Tests both that your pager is working and that the dialup service provider is configured correctly.

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



A test page is being sent to 5551212 at test2.

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**.

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 CHAPTER Setting up Event Filters

Setting up Event Filters is for Administrator accounts only.

You can configure Network Discovery to notify you when events occur. Network Discovery can notify you by e-mail, by pager, or by SNMP trap, and can even open a ticket in Peregrine ServiceCenter. 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

The most important thing to remember about event filters is that they rely on the system-level device priorities which are controlled by Administrator and IT Manager accounts. In order for your event filters to work properly, you must make sure you set the system-level priorities for your devices properly.

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 *User Guide*.

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 *Network Discovery Setup Guide*.
Events Issues	
Understand the types of events recorded by Network Discovery	See *The Events Browser* on page 79 and the *Reference Manual*.
Understand how to configure Network Discovery to send tickets to ServiceCenter	See *Using Network Discovery with ServiceCenter and AssetCenter* on page 169.
Hardware Issues	
Set up and test your pager equipment (hardware and software)	See *Setting up Paging* on page 137.
Account Issues	
Set up account contact information	**Administration > Account administration > Account properties.** See *Modifying account contact information* on page 32.
Network Map Issues	

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

Concept	Commands and where to get more information
Change device priorities	*Changing Device Properties* on page 110
Changing alarm thresholds	*Changing Alarm Thresholds* on page 112

Event filters are an advanced option. You have the power to send pager and e-mail messages whenever a device attribute 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?

All events in the network are recorded in the event log. You can select events that are important to you, and Network Discovery can notify you in the following ways:

- 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
- open a ticket in Peregrine ServiceCenter

Network Discovery has two default event filters. You can create your own through **Administration** > **Event Filters**.

You can enter a range of IP addresses if you want to be alerted about events on a portion of your network. This allows you to create event filters specifically for a network, subnet, or even a single device. If you leave this section blank, the event filter will apply to all devices in your network.

You can also add a “notification delay.” This means that when an event occurs, Network Discovery will wait the specified amount of time before notifying the user. Sometimes, events will be rectified on their own. If the problem is automatically rectified within the notification delay period, the user will not be notified.

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.

[a] The “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:
  - SMTP server
  - SNMP traps setup (only if you plan to use SNMP traps)
  - Pager setup (hardware installation and pager service provider information)
  - ServiceCenter configuration
- 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 you have set the system-level priority for your important devices.
- Set up the proper alarm thresholds.

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

Event Filter Properties

The properties of event filters are as follows:

Property	Explanation
Name	The name can be 3-20 characters long, can include lower case letters, numbers, underscore (_), and hyphen (-). The underscore and hyphen cannot be the first character.
Description	The description can be 0-60 characters long; used to provide a reminder as to the purpose of the filter.
Event Type	You have a choice of several types of events for which you want to receive notification. ■ All (all of the categories listed below) ■ Attributes (when an attribute is in an alarmed state, all of which are available in the second list in the Event Filter menu: Load Average, CPU, Memory, etc.) ■ Adds (when a device is added in your specified IP range) ■ Deletes (when a device is deleted in your specified IP range) ■ Property (when you change a device property for the type of device specified in your IP range, like an icon, device priority, device tag, or device title) ■ Moves (when there is a connectivity change within your IP range, i.e., a changed port, or when devices are physically moved and connected differently; indicated by a *Port Moves* event in the Health Panel) **Note:** The safest and easiest way to make sure you get your event notification is to select the *All* Event Type category. That way, you will be notified if any of these categories has an event occur. However, if you want to receive notification for a very specific event, you should pick an event type.
Attribute Group	If you have chosen *Attributes* as your Event Type, you can choose one of these attribute groups.
Priority	The priority of devices about which you want to be notified.
Device Type	The type of device about which you want to be notified.
Line Alarm Type (only for Line Event Filters)	The type of lines about which you want to be notified.

Property	Explanation
State Transition	If you want to be notified about specific state transitions, you can select them here. Click one state in the *From* category, and one from the *To* category and click **Add**. **Note:** The "Info" transition comprises Adds and Deletes
IPv4 Range	Enter a range of IPv4 addresses in which you want to be notified of this event.
Notification	Notifications must include an action, and can include an account. You can also add a *Delay*, so if the event corrects itself within the Delay period, no notification will be sent. ■ send e-mail ■ send alphanumeric page directly to pager ■ send alphanumeric page via e-mail gateway ■ send SNMP trap data ■ open a ticket in ServiceCenter

Examples of common Event Filters

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

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

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

Example 1: Notification when a core device breaks

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

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

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

To set up the Administrator account

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

To set the device priority

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

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

To set up the event filter

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

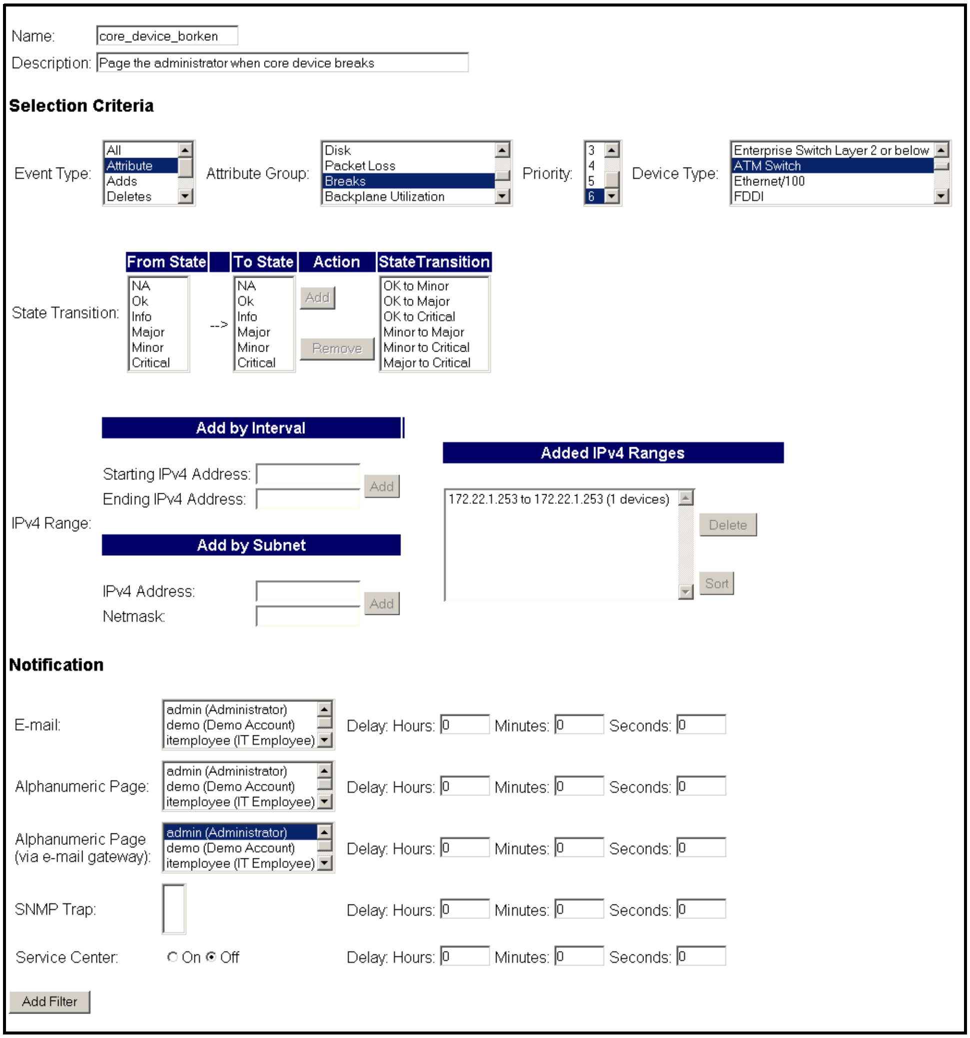
Field	Enter:
Name (create a name for the filter)	core_device_broken
Description	Page administrator when core device breaks
Event Type	Attribute
Attribute Group	Breaks
Priority	6
Device Type	ATM Switch
Transitions	OK to Minor, OK to Major, OK to Critical, Minor to Major, Minor to Critical, Major to Critical

Field	Enter:
IPv4 Range	Select the devices or IP range you want this event filter to monitor
Alphanumeric Page	Select the Administrator account

3 You can have Network Discovery delay the notification by entering a time in the Delay section of the notification table.

4 Click **Add Filter.**

Figure 11-1: Example of a Device Event Filter



Name: core_device_borken

Description: Page the administrator when core device breaks

Selection Criteria

Event Type: All, Attribute (selected), Adds, Deletes

Attribute Group: Disk, Packet Loss, Breaks (selected), Backplane Utilization

Priority: 3, 4, 5, 6 (selected)

Device Type: Enterprise Switch Layer 2 or below, ATM Switch (selected), Ethernet/100, FDDI

State Transition:

From State		To State	Action	StateTransition
NA Ok Info Major Minor Critical	-->	NA Ok Info Major Minor Critical	Add Remove	OK to Minor OK to Major OK to Critical Minor to Major Minor to Critical Major to Critical

IPv4 Range:

Add by Interval

Starting IPv4 Address:

Ending IPv4 Address:

Add by Subnet

IPv4 Address:

Netmask:

Added IPv4 Ranges

172.22.1.253 to 172.22.1.253 (1 devices)

Notification

E-mail:	admin (Administrator) demo (Demo Account) itemployee (IT Employee)	Delay: Hours: 0	Minutes: 0	Seconds: 0
Alphanumeric Page:	admin (Administrator) demo (Demo Account) itemployee (IT Employee)	Delay: Hours: 0	Minutes: 0	Seconds: 0
Alphanumeric Page (via e-mail gateway):	admin (Administrator) (selected) demo (Demo Account) itemployee (IT Employee)	Delay: Hours: 0	Minutes: 0	Seconds: 0
SNMP Trap:		Delay: Hours: 0	Minutes: 0	Seconds: 0
Service Center:	○ On ● Off	Delay: Hours: 0	Minutes: 0	Seconds: 0

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

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

To set up the Administrator account

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

To set the device priority

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

   If you want to set this up for several routers, then repeat these steps for each router. Note their IPv4 addresses if you want to specify the IPv4 range.
7. Set the Packet Loss thresholds by clicking **Edit** > **Alarm Thresholds**.
8. Click **Apply**.
9. Click **OK**.

To set up the Event Filter

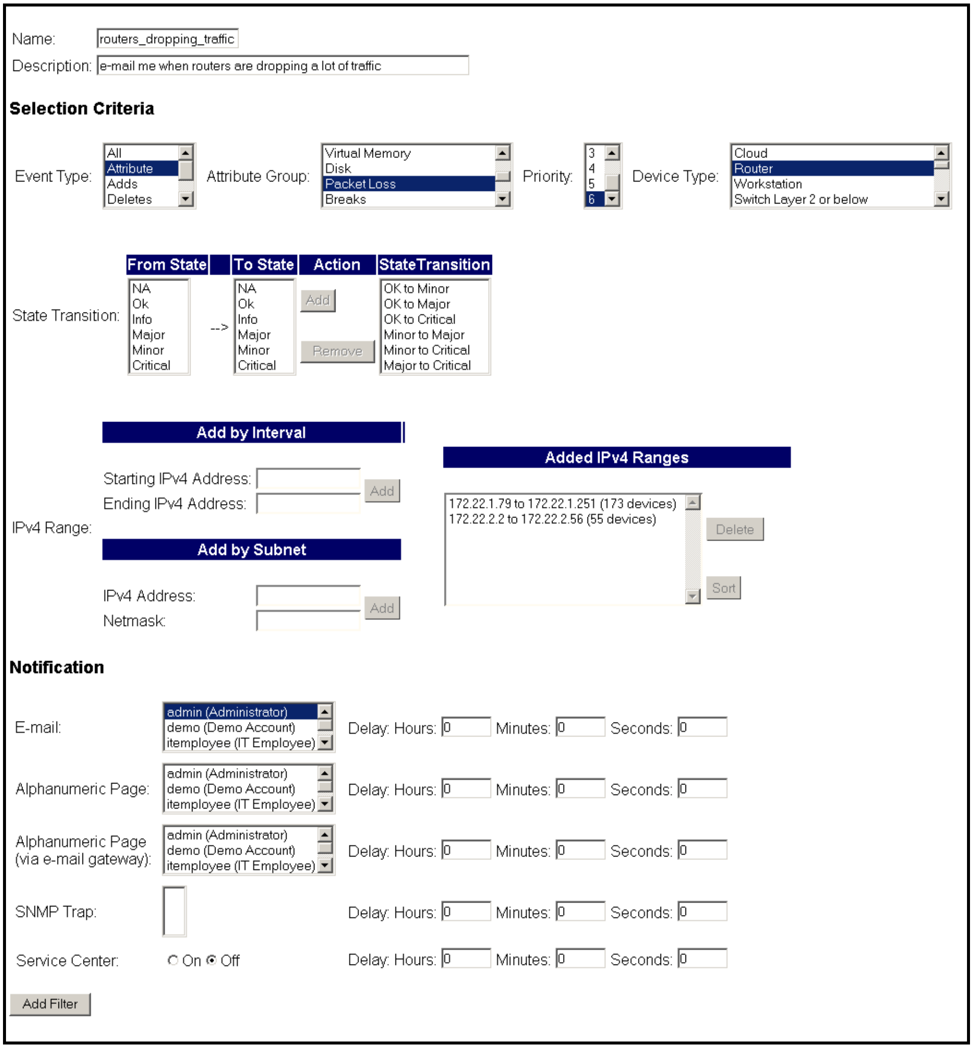
1. Click **Administration** > **Event filter configuration** > **Add a device filter**.
2. Enter the event filter information as it appears in this table:

Field	Enter:
Name (create a name for the filter)	routers_dropping_traffic
Description	E-mail me when routers are dropping a lot of traffic
Event Type	Attribute

Field	Enter:
Attribute Group	Packet Loss
Priority	6
Transitions	OK > Minor, OK > Major, OK > Critical, Minor > Major, Minor > Critical, Major > Critical
Device Type	Router
E-mail	select the Administrator account
IPv4 Range	Select the devices or IP range you want this event filter to monitor

3 Click Add Filter.

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



Name: routers_dropping_traffic

Description: e-mail me when routers are dropping a lot of traffic

Selection Criteria

Event Type: All, Attribute (selected), Adds, Deletes

Attribute Group: Virtual Memory, Disk, Packet Loss (selected), Breaks

Priority: 3, 4, 5, 6 (selected)

Device Type: Cloud, Router (selected), Workstation, Switch Layer 2 or below

State Transition:

From State	To State	Action	StateTransition
NA Ok Info Major Minor Critical	NA Ok Info Major Minor Critical	Add Remove	OK to Minor OK to Major OK to Critical Minor to Major Minor to Critical Major to Critical

IPv4 Range:

Add by Interval

Starting IPv4 Address:
Ending IPv4 Address:

Add by Subnet

IPv4 Address:
Netmask:

Added IPv4 Ranges

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

Notification

E-mail:	admin (Administrator) (selected) demo (Demo Account) itemployee (IT Employee)	Delay: Hours: 0 Minutes: 0 Seconds: 0
Alphanumeric Page:	admin (Administrator) demo (Demo Account) itemployee (IT Employee)	Delay: Hours: 0 Minutes: 0 Seconds: 0
Alphanumeric Page (via e-mail gateway):	admin (Administrator) demo (Demo Account) itemployee (IT Employee)	Delay: Hours: 0 Minutes: 0 Seconds: 0
SNMP Trap:		Delay: Hours: 0 Minutes: 0 Seconds: 0
Service Center:	○ On ● Off	Delay: Hours: 0 Minutes: 0 Seconds: 0

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

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

To set up the Administrator account

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

To set the device priority

1. Open a Network Map session.
2. Find your server and select it.
3. Click **Object** > **Device Properties**.
4. In the Device Properties window, make this Server priority 6.

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

   If you want to be paged for several servers, repeat steps 2-6 for each server.
7. Set the Line Alarm thresholds by clicking **Edit** > **Alarm Thresholds**.
8. Click **Apply**.
9. Click **OK**.

To set up the Event Filter

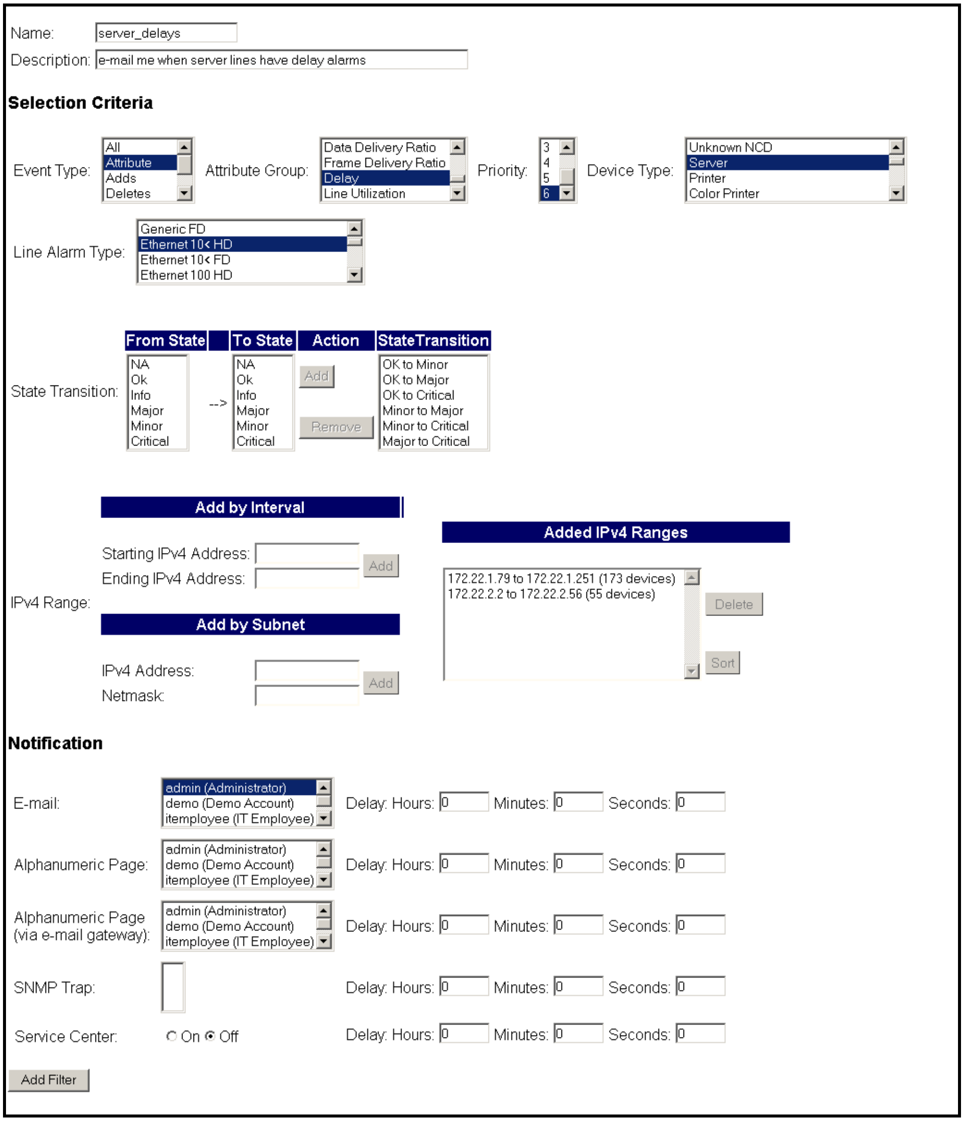
1. Click **Administration** > **Event filter configuration** > **Add a line filter**.

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

Field	Enter:
Name (create a name for the filter)	server_delays
Description	E-mail me when server lines have Delay alarms
Event Type	Attribute
Attribute Group	Delays
Priority	6
Device Type	Server
Line Alarm Type	Ethernet 10< HD
Transitions	OK > Minor, OK > Major, OK > Critical, Minor > Major, Minor > Critical, Major > Critical
E-mail	select the Administrator account
IPv4 Range	Select the devices or IP range you want this event filter to monitor

3 Click **Add Filter.**

Figure 11-3: Example of a Line Event Filter



Name: server_delays

Description: e-mail me when server lines have delay alarms

Selection Criteria

Event Type: All, **Attribute**, Adds, Deletes

Attribute Group: Data Delivery Ratio, Frame Delivery Ratio, **Delay**, Line Utilization

Priority: 3, 4, 5, **6**

Device Type: Unknown NCD, **Server**, Printer, Color Printer

Line Alarm Type: Generic FD, **Ethernet 10< HD**, Ethernet 10< FD, Ethernet 100 HD

State Transition:

From State		To State	Action	StateTransition
NA Ok Info Major Minor Critical	-->	NA Ok Info Major Minor Critical	Add Remove	OK to Minor OK to Major OK to Critical Minor to Major Minor to Critical Major to Critical

IPv4 Range:

Add by Interval

Starting IPv4 Address: Add

Ending IPv4 Address:

Add by Subnet

IPv4 Address: Add

Netmask:

Added IPv4 Ranges

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

Delete

Sort

Notification

E-mail:	**admin (Administrator)** demo (Demo Account) itemployee (IT Employee)	Delay: Hours: 0	Minutes: 0	Seconds: 0
Alphanumeric Page:	admin (Administrator) demo (Demo Account) itemployee (IT Employee)	Delay: Hours: 0	Minutes: 0	Seconds: 0
Alphanumeric Page (via e-mail gateway):	admin (Administrator) demo (Demo Account) itemployee (IT Employee)	Delay: Hours: 0	Minutes: 0	Seconds: 0
SNMP Trap:		Delay: Hours: 0	Minutes: 0	Seconds: 0
Service Center:	○ On ● Off	Delay: Hours: 0	Minutes: 0	Seconds: 0

Add Filter

Example 4: Open a ticket in ServiceCenter when an important device breaks

For this example, we will set up an event filter that will open a ticket in ServiceCenter when a device of priority 4-6 breaks. You may have several devices in your network set to these priority levels. This event filter will work for all of those devices.

Before you start the procedure, make sure your ServiceCenter configuration is correct (see *Using Network Discovery with ServiceCenter and AssetCenter* on page 169).

To set the device priority

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

   You have now changed the priority of your core device to 6.
7. If you want ServiceCenter tickets to be opened for several devices, repeat step 1 to step 6 for each device.

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:

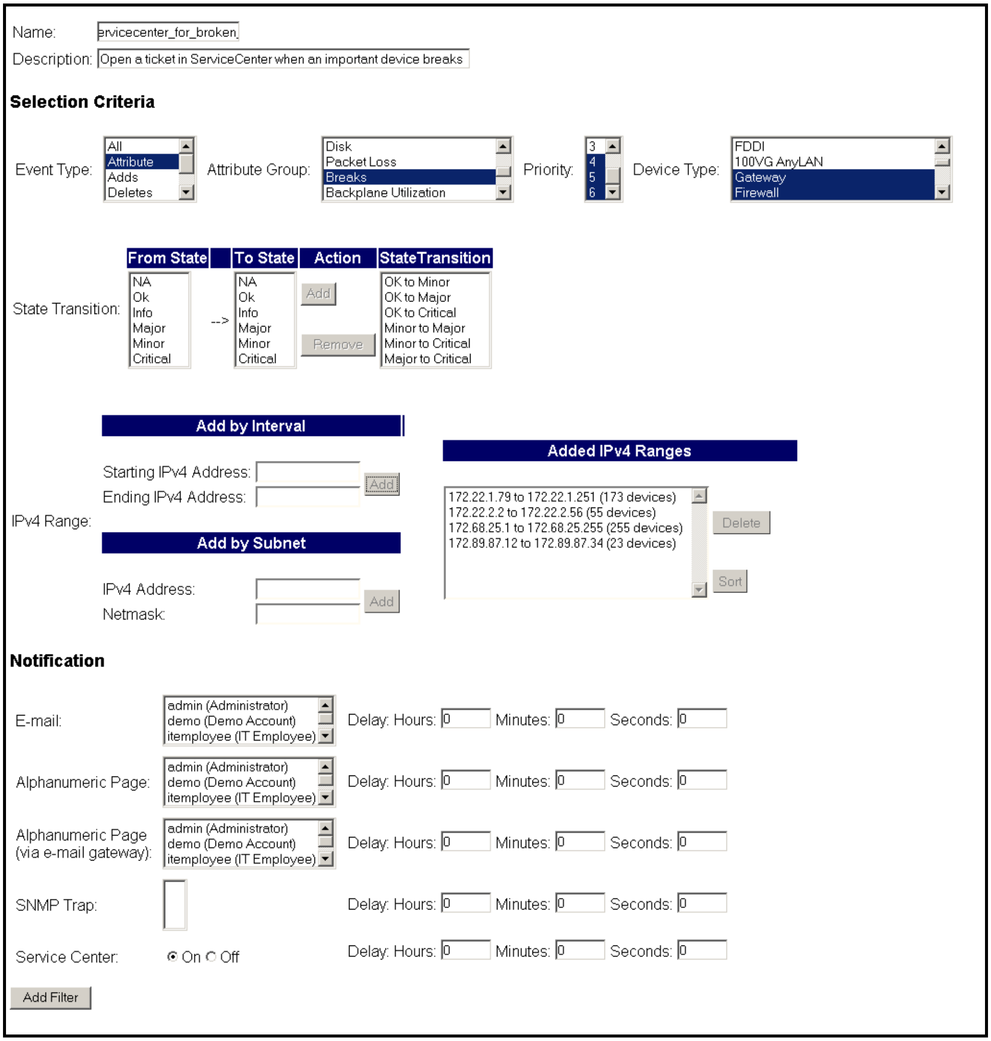
Field	Enter:
Name (create a name for the filter)	servicecenter_for_broken_device
Description	Open a ServiceCenter ticket when an important device breaks
Event Type	Attribute
Attribute Group	Breaks
Priority	6
Device Type	ATM Switch, Router, Gateway, Firewall

Field	Enter:
Transitions	OK to Minor, OK to Major, OK to Critical, Minor to Major, Minor to Critical, Major to Critical
IPv4 Range	Select the devices or IP range you want this event filter to monitor
ServiceCenter	Click “On”

3 You can have Network Discovery delay the notification by entering a time in the Delay section of the notification table.

4 Click **Add Filter**.

Figure 11-4: Example of a Device Event Filter



Name: ervicecenter_for_broken

Description: Open a ticket in ServiceCenter when an important device breaks

Selection Criteria

Event Type: All / Attribute / Adds / Deletes (selected: Attribute)

Attribute Group: Disk / Packet Loss / Breaks / Backplane Utilization (selected: Breaks)

Priority: 3 / 4 / 5 / 6 (selected: 4, 5, 6)

Device Type: FDDI / 100VG AnyLAN / Gateway / Firewall (selected: Gateway, Firewall)

State Transition:

From State		To State	Action	StateTransition
NA Ok Info Major Minor Critical	-->	NA Ok Info Major Minor Critical	Add Remove	OK to Minor OK to Major OK to Critical Minor to Major Minor to Critical Major to Critical

IPv4 Range:

Add by Interval

Starting IPv4 Address:

Ending IPv4 Address:

Add by Subnet

IPv4 Address:

Netmask:

Added IPv4 Ranges

172.22.1.79 to 172.22.1.251 (173 devices)
172.22.2.2 to 172.22.2.56 (55 devices)
172.68.25.1 to 172.68.25.255 (255 devices)
172.89.87.12 to 172.89.87.34 (23 devices)

Notification

E-mail:	admin (Administrator) demo (Demo Account) itemployee (IT Employee)	Delay: Hours: 0	Minutes: 0	Seconds: 0
Alphanumeric Page:	admin (Administrator) demo (Demo Account) itemployee (IT Employee)	Delay: Hours: 0	Minutes: 0	Seconds: 0
Alphanumeric Page (via e-mail gateway):	admin (Administrator) demo (Demo Account) itemployee (IT Employee)	Delay: Hours: 0	Minutes: 0	Seconds: 0
SNMP Trap:		Delay: Hours: 0	Minutes: 0	Seconds: 0
Service Center:	● On ○ Off	Delay: Hours: 0	Minutes: 0	Seconds: 0

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 Type list box.
2. Select one or more options from the Attribute Group list box.
3. Select one or more options from the Priority list box.
4. Select one or more options from the Device Type list box.
5. Select one or more options from the Line Alarm list box.
6. Select one or more options from the State Transitions list box.

Note: These selection criteria apply to all notifications.

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

▶ Select the appropriate notification for the event filter:

- E-mail
- Alphanumeric Page
- Alphanumeric Page (through e-mail gateway)
- SNMP Trap
- ServiceCenter ticket

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

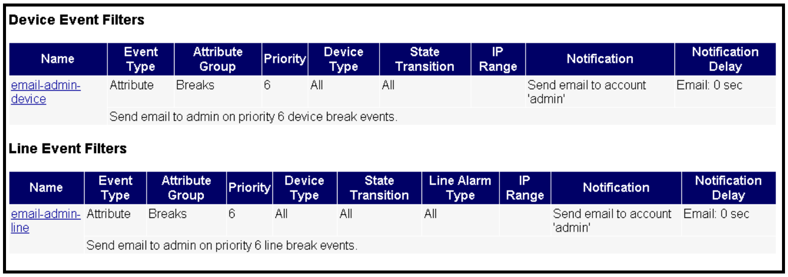
The filter names are hyperlinked. Clicking the hyperlinks will take you to the *Modifying a filter* page for that filter.

To list filters

1 Click **Administration** > **Event filter configuration** > **List filters.**

2 Click a filter name hyperlink.

Figure 11-5: List Event Filters (default event filters shown)



Device Event Filters

Name	Event Type	Attribute Group	Priority	Device Type	State Transition	IP Range	Notification	Notification Delay
email-admin-device	Attribute	Breaks	6	All	All		Send email to account 'admin'	Email: 0 sec
	Send email to admin on priority 6 device break events.							

Line Event Filters

Name	Event Type	Attribute Group	Priority	Device Type	State Transition	Line Alarm Type	IP Range	Notification	Notification Delay
email-admin-line	Attribute	Breaks	6	All	All	All		Send email to account 'admin'	Email: 0 sec
	Send email to admin on priority 6 line break events.								

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 CHAPTER Using Network Discovery with ServiceCenter and AssetCenter

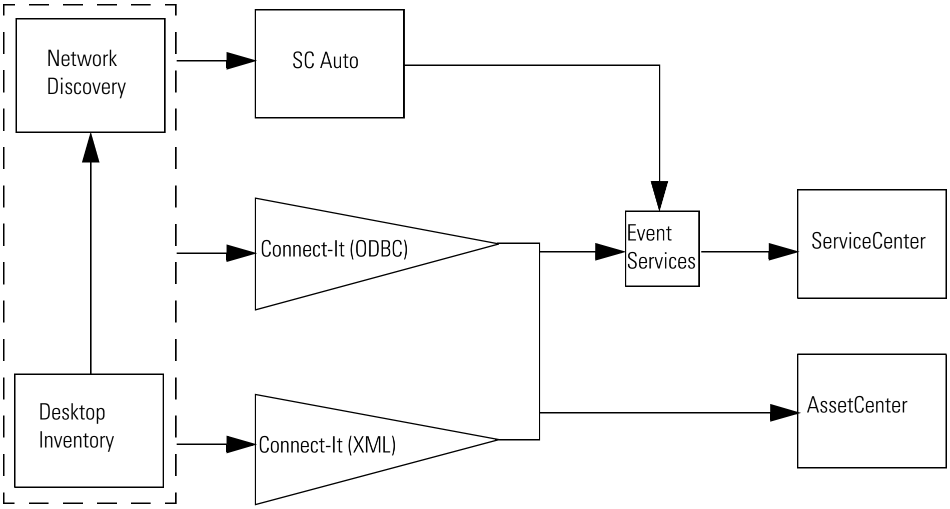
Most Peregrine products can work together. When working with Network Discovery, there are many ways to integrate data with other Peregrine products such as:

- Desktop Inventory
- Desktop Administration
- ServiceCenter (using Connect-It or SCAuto)
- AssetCenter (using Connect-It)

This chapter will discuss ServiceCenter and AssetCenter. For information on the other products, refer to *Using Network Discovery with Desktop Inventory and Desktop Administration*.

Sharing data with ServiceCenter and AssetCenter

Figure 12-1: Peregrine product interaction



The main goal for passing any data from Network Discovery/Desktop Inventory to ServiceCenter or AssetCenter is to have an accurate list of all the devices and assets in your network. When this list is created manually, it will become outdated quickly. It is best to have the list automatically created and updated through the database.

You can use Connect-It to pass data from the Network Discovery database to the AssetCenter or ServiceCenter server. This will allow you to always have up-to-date information on:

- the state of the network and all devices
- the precise components in a given device (network card, CPU, RAM, and so on)
- the configuration of leased devices (for example, keeping track of the original configuration of the device, so any changes are accounted for)
- what devices have been removed from the network

In addition, Desktop Inventory offers software tracking to help with:

- site license information
- managing software installation on a given computer

- upgrading and monitoring software versions
- upgrading and monitoring OS

Using the SCAuto update method allows Network Discovery to offer the following:

- automatic ticketing in case of failure
- inventory information as changes occur in the network monitored by Network Discovery

ServiceCenter uses its SCAuto and Event Services features to track events automatically generated from external sources (such as Network Discovery and other network management products). You must set up your ServiceCenter Event Services to properly receive the data sent from Network Discovery.

To set up and use ServiceCenter and Event Services properly, see your ServiceCenter documentation. The rest of this chapter will outline how to set up Network Discovery for use with ServiceCenter.

To set up and use AssetCenter properly, see your AssetCenter documentation.

Copying the Network Discovery database

Directly from Network Discovery

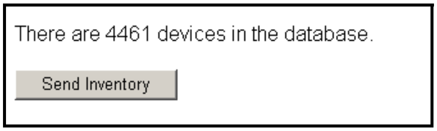
Once you have set up your access to ServiceCenter (see *Configure access to ServiceCenter* on page 175), you can export the Network Discovery inventory to ServiceCenter using the **Send Inventory** command. Depending on the size of your inventory, it may take up to an hour to transmit all the data.

The Send Inventory command initiates a series of Add events, which will populate the ServiceCenter database.

To send your inventory data to ServiceCenter

1. Click **Administration** > **Data management** > **Send Inventory**.
2. Click **Send Inventory**.

Figure 12-2: ServiceCenter configuration



There are 4461 devices in the database.

With Connect-It

Network Discovery, ServiceCenter, and AssetCenter store their information in databases. Using Connect-It, you can pass network data between Network Discovery and ServiceCenter and/or AssetCenter. Connect-It uses its “scenarios” to read the tables and entries in the Network Discovery database, and translate it to similar tables and entries in the other products.

Note: If data from Network Discovery and Desktop Inventory is combined in the Network Discovery database, Desktop Inventory data info is given higher priority for most types of data. For example, there may be two definitions for the System Location entry. If Network Discovery says “2nd floor” and Desktop Inventory says “3rd floor,” then the winning data in ServiceCenter will be “3rd floor.”

For more information on how to set up Connect-It scenarios, see your Connect-It documentation.

Data Export Using ODBC

If you are using Network Discovery with ServiceCenter or any other applications, you can export the Network Discovery database using ODBC.

See the *Data Export Guide* for more information, and also see the **Help** > **Database schema** link in Network Discovery to see how the database is organized.

Using Network Discovery with ServiceCenter

Important: This feature will only work with Network Discovery version 5.1 (or later), and ServiceCenter version 5.1 (or later).

Events in Network Discovery and ServiceCenter

You can use Connect-It or ODBC to initially populate the ServiceCenter database with your Network Discovery data. After that, you can use Network Discovery and ServiceCenter to update the ServiceCenter database when the network changes. In addition, you can use the two products to automatically open and close ServiceCenter tickets.

To open and close tickets in ServiceCenter, Network Discovery sends two types of event register records to ServiceCenter (through Event Services).

ServiceCenter Event	Explanation
NDpmo	Open an Incident Management ticket in ServiceCenter.
NDpmc	Close an Incident Management ticket in ServiceCenter.

Note: The NDpm events are processed immediately by ServiceCenter, so the ticket can be opened/closed quickly.

These same events will pass back from ServiceCenter to Network Discovery as confirmation messages when a ticket is opened or closed.

Opening Tickets in ServiceCenter

Note: In order to automatically open tickets in ServiceCenter, you must have your event filters set up properly (see *Setting up Event Filters* on page 147).

When a network problem occurs, and a Network Discovery event filter is triggered, an NDpmo event is sent to Event Services, and then a ticket is opened in ServiceCenter. Another NDpmo event is sent back to Network Discovery, which contains the ticket information (see *Where you see ServiceCenter data* on page 175).

When that network problem is returned to an OK state, the ticket is automatically closed using the NDpmc event.

Note: If someone manually closes the ticket in ServiceCenter, the ticket will still appear open in Network Discovery. The ticket will only appear closed when Network Discovery sees the problem return to an OK state.

Note: To see the history of a ticket, or to perform any further customization, you must access the data through ServiceCenter. See your ServiceCenter documentation for more information.

Where you see ServiceCenter data

There are several places to see ServiceCenter ticket numbers in Network Discovery.

- Device Manager State panel (a Ticket column will appear if there are tickets open)
- Port Manager State panel
- Attribute Manager Configuration panel
- Health Panel category/Alarms Viewer
- Network Map pop-up information
- Service Analyzer pop-up information

Note: A pop-up will show up to three tickets for a device.

A pop-up will not show the tickets if you are in Forecast mode (see *Checking the Network Forecast* on page 72).

Configure access to ServiceCenter

You must configure Network Discovery to communicate with ServiceCenter if you are to have tickets automatically created.

To configure access to ServiceCenter

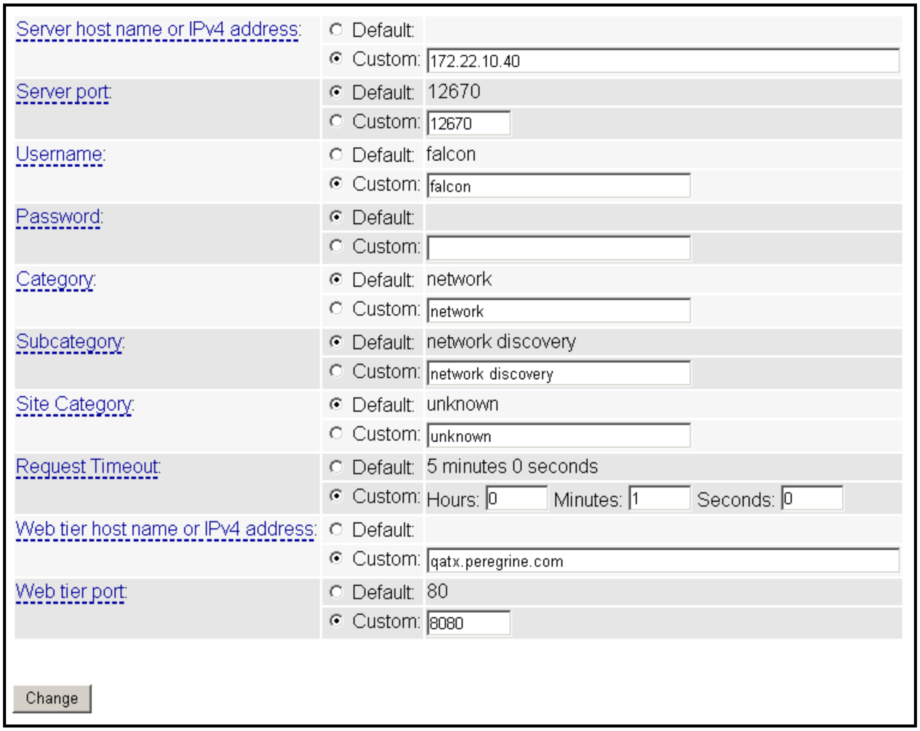
1. Click **Administration** > **System preferences** > **ServiceCenter configuration.**
2. Enter the settings for your ServiceCenter configuration.

Setting	Explanation
Server Host name of IPv4 address	The address of your ServiceCenter product.
Server Port	The port for accessing ServiceCenter.
Username	Your ServiceCenter account name.
Password	Your ServiceCenter account password.
Request Timeout	Optional.
Category, Subcategory, Site Category	These are required fields in ServiceCenter tickets.

Setting	Explanation
Web tier host name of IPv4 address	The host name or IPv4 address of the server that will allow you direct access to ServiceCenter tickets.
Web tier port	The port through which Network Discovery can access ServiceCenter tickets.

3 Click **Change.**

Figure 12-3: ServiceCenter configuration



Server host name or IPv4 address:	○ Default:	
	● Custom:	172.22.10.40
Server port:	● Default:	12670
	○ Custom:	12670
Username:	○ Default:	falcon
	● Custom:	falcon
Password:	● Default:	
	○ Custom:	
Category:	● Default:	network
	○ Custom:	network
Subcategory:	● Default:	network discovery
	○ Custom:	network discovery
Site Category:	● Default:	unknown
	○ Custom:	unknown
Request Timeout:	○ Default:	5 minutes 0 seconds
	● Custom:	Hours: 0 Minutes: 1 Seconds: 0
Web tier host name or IPv4 address:	○ Default:	
	● Custom:	qatx.peregrine.com
Web tier port:	○ Default:	80
	● Custom:	8080

Configure the Appliance ID

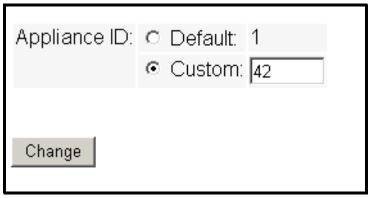
The ID of your Peregrine appliance. If you have more than one Peregrine appliance in your network, you need to give each appliance a distinct ID to help ServiceCenter determine the source of the ticket.

Failure to give each appliance its own ID will result in tickets being updated with updates from multiple Peregrine appliances.

You must also set the Appliance ID

1. Click **Administration** > **System preferences** > **Aggregate configuration**.
2. Enter an appliance ID.
3. Click Change.

Figure 12-4: Appliance ID



Appliance ID: ○ Default: 1
● Custom: 42

Test your Connection to ServiceCenter

To test your connection to ServiceCenter

1. Click **Administration** > **Data management** > **Test ServiceCenter connection.**
2. Click **Test ServiceCenter.**

   A message appears, confirming your connection, or warning you that your settings are not correct.

Note: If your connection to ServiceCenter goes down, you will see an alarm in **Status** > **Appliance Health** > **Software Modules** > **Event Notifier via ServiceCenter** as the pending events accumulate.

Deleting your ServiceCenter tickets

You may want to delete all the tickets opened by Network Discovery if you:

- have been performing tests between Network Discovery and ServiceCenter, and want to ensure all the test tickets are closed.
- move from a test version to a production version of ServiceCenter

Note: You cannot delete individual tickets.

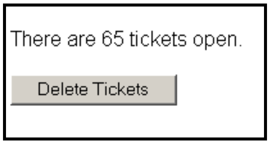
Note: This procedure does not close tickets in ServiceCenter.

To delete all the ServiceCenter tickets opened by Network Discovery

1 Click **Administration** > **Data management** > **Delete tickets.**

2 Click **Delete Tickets.**

Figure 12-5: Deleting Tickets



There are 65 tickets open.

13 CHAPTER Adding and Replacing Devices

There will be many situations when you are adding 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

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.

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**.
5. From the pull-down list, select **Query Network**.
6. Click **Update**.

Network Discovery begins network discovery on the device immediately.

With the same IP Address as an active device

If you add a new device to the network that has the same IP address as an active device, the old device will automatically be moved to the list of Deactivated Devices (**Status** > **Deactivated Devices**). You will also see an exception for the old device, stating that the device has been deactivated because of a “duplicate IP address.”

With the same IP Address as a deactivated device

If a device has been deactivated (either manually by the user, or automatically by Network Discovery), and you add a new device with the same IP address, there will not be a “duplicate IP address” exception.

However, if the deactivated device becomes reactivated (either manually by the user or it is rediscovered by Network Discovery), there will be a “duplicate IP address” exception. At that point, the newly reactivated device will remain on the map, and the other device will be deactivated.

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 different MAC and IP addresses, it is best to purge the old device manually. This ensures that the device model for your new device is not merged with the model of the old device.

Note: Priorities from “replaced” devices are not automatically assigned to “new” devices. If the Administrator manually changed the priority of the old device, and you are introducing a new device with the same IP address as the old device, make sure you manually change the priority of the new device. This will ensure correct event notification.

With a different device

When you replace a device with a different device and a unique IP address, 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.

Purging Devices

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** > **Visibility** > **Purge**.

   A confirmation message appears.
4. Click **OK**.

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

1. Click the **Device Visibility** button.
2. Select **Purge** from the pull-down list.
3. Click **Purge**.

To purge a port from a device

1. In the Port Manager, click the **Purge port** button.

   A confirmation message appears.
2. Click **Purge**.

Activating devices

This command will bring a device from the list of deactivated devices, back onto the network map. Network Discovery will start monitoring this device again.

Note: You can re-activate devices if they have been deactivated or hidden by Network Discovery, or by an Administrator.

For information on how to Hide, Purge, or Deactivate devices, see *Removing devices* on page 192.

To reactivate a device from the hidden list

1. Click **Status** > **Hidden Devices**.
2. Click on the device title.

   A Device Manager will open for that hidden device.

3 Click the Device Visibility button.

4 Select “Activate” from the pull-down list.

5 Click **Activate**.

The device should return to the Network Map, and Network Discovery will begin to monitor this device again.

To reactivate a device from the deactivated list

1 Click **Status** > **Deactivated Devices**.

2 Click on the device title.

A Device Manager will open for that deactivated device.

3 Click the Device Visibility button.

4 Select “Activate” from the pull-down list.

5 Click **Activate**.

The device should return to the Network Map, and Network Discovery will begin to monitor this device again.

14 CHAPTER Deleting Data, Connections, and 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 deactivation and purge intervals, you risk removing devices from your network that would not be removed with the default settings.

Topics in this chapter include:

- *Deleting data* on page 188
- *Deleting connections* on page 190
- *Removing devices* on page 192

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 *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

Important: If you are working on an Aggregator appliance (see *Using an Aggregator* on page 197), you can only delete the data native to the Aggregator. To delete the data associated with a remote appliance, you must delete the remote appliance. For more information, see *Deleting Remote Appliances* on page 210.

Table 14-1: Options for deleting data

What gets deleted	Network data	Network data plus accounts	Network data, accounts, config, backups
Devices for this appliance	✓	✓	✓
Events	✓	✓	✓
Forecast databases	✓	✓	✓
Accounts	—	✓	✓
Map configurations	—	✓	✓
Devices for any remote appliances[a]	—	—	✓
Administration configuration	—	—	✓
Internal backups	—	—	✓

[a] This applies only when an Aggregator license is present.

To delete Network Discovery data

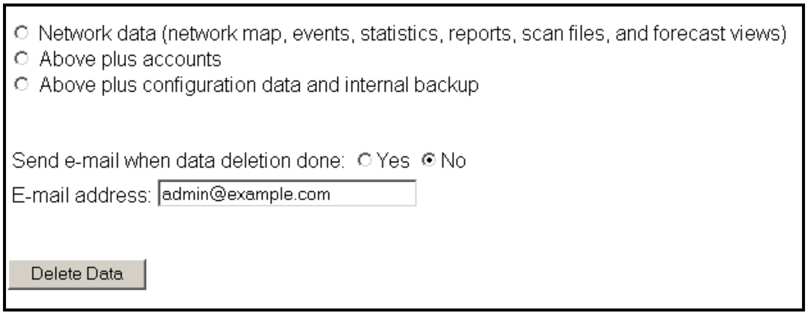
1 Click **Administration** > **Data management** > **Delete data.**

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: admin@example.com

Deleting connections

This procedure will delete connections between objects on the Network Map. It will take a few minutes 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.

Warning: You can potentially lose all the connectivity data Network Discovery has gathered.

Warning: This action cannot be undone.

To delete all connections

1 Click **Administration** > **Data management** > **Delete connections.**

2. Click **All.**
3. Click **Delete Connections.**
4. Click **Confirm.**

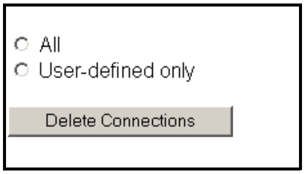
Both automatic and user-defined connections are deleted.

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



Removing devices

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

Table 14-2: Device removal methods

Method	Performed by	How it works
automatic	Network Discovery	3 stages ■ deactivate ■ purge ■ obliterate
manual	an IT Manager or Administrator user	3 methods ■ hide ■ deactivate ■ purge

Table 14-3: Comparing hide, deactivate, purge, and obliterate

Action	Hide	Deactivate	Purge	Obliterate[a]
device removed from Network Map	✓	✓	✓	✓
device can be recovered if seen	—	✓	✓[b]	—[b]
“delete” event generated	✓	✓	✓	—
device statistics deleted	—	—	✓	✓
device events deleted from Events Browser	—	—	✓	✓
device events deleted from Reports Database	—	—	—	✓

[a] Devices cannot be manually obliterated.
[b] Once removed from the Reports Database, a device can still be rediscovered, but it will be considered a new device.

Removing devices automatically

The automatic removal process begins once Network Discovery detects that a device has not been seen. The deactivation interval begins as soon as a device is discovered, and restarts after every model update. When the deactivation interval ends, the device is made inactive.

A deactivation interval refers to the length of time Network Discovery will wait before it makes a “not seen” device inactive. The deactivation 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.

Note: There is limited space for deactivated devices. Once this capacity is exceeded, devices are purged, regardless of the deactivation interval. The number of devices that can be deactivated at one time is 10% of the device license for the Peregrine appliance.

When the device is inactive, it is considered “deactivated” and appears in the list of devices at **Status** > **Deactivated Devices**. Once the device is inactive, the purge interval begins. When the device is set to be purged, one of two things can happen:

- If your device license capacity is full, the purged device will be obliterated, meaning that the device and all its associated data will be removed from the database.
- If there is space in the database, the purged device will remain in the database until the obliteration interval passes.

Note: The number of purged devices that Network Discovery keeps depends on your license. For example, if you have a 10,000 device license, with 8,000 active devices in your network, Network Discovery will be able to keep records for 2,000 purged devices. However, active devices always take precedence over purged devices. If you have 10,000 active devices, Network Discovery will not save any purged devices in its database.

Changing the device expiry intervals

Device expiry has three steps: deactivation, purge, and obliteration.

Changing the expiry intervals

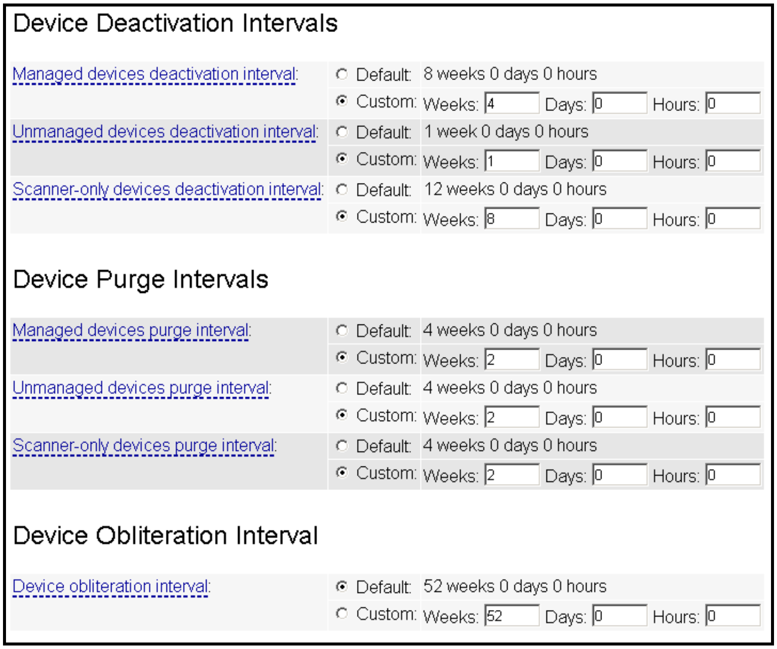
For deactivation and purge, there are three intervals, one each for devices with:

- SNMP management
- no SNMP management
- Scanner-only devices (if available in your network)

Whether or not the deactivation interval is accepted depends on your Device Modeler Interval.

The obliteration interval is the same for all devices.

Figure 14-3: Device Deactivation, Purge, and Obliteration Intervals



Device Deactivation Intervals

Managed devices deactivation interval:	○ Default:	8 weeks 0 days 0 hours
	● Custom:	Weeks: 4 Days: 0 Hours: 0
Unmanaged devices deactivation interval:	○ Default:	1 week 0 days 0 hours
	● Custom:	Weeks: 1 Days: 0 Hours: 0
Scanner-only devices deactivation interval:	○ Default:	12 weeks 0 days 0 hours
	● Custom:	Weeks: 8 Days: 0 Hours: 0

Device Purge Intervals

Managed devices purge interval:	○ Default:	4 weeks 0 days 0 hours
	● Custom:	Weeks: 2 Days: 0 Hours: 0
Unmanaged devices purge interval:	○ Default:	4 weeks 0 days 0 hours
	● Custom:	Weeks: 2 Days: 0 Hours: 0
Scanner-only devices purge interval:	○ Default:	4 weeks 0 days 0 hours
	● Custom:	Weeks: 2 Days: 0 Hours: 0

Device Obliteration Interval

Device obliteration interval:	● Default:	52 weeks 0 days 0 hours
	○ Custom:	Weeks: 52 Days: 0 Hours: 0

To change the expiry intervals

1 Click **Administration** > **System Preferences** > **Expiry.**

2 Enter the time values deactivation, purge, and obliteration.

3 Click **Change**.

Removing devices manually

The manual removal process can occur in three ways. An Administrator can Deactivate, Hide, or Purge a device.

By using these commands, you are *not* making a physical change to the device or network. The manual removal of a device from the Network Map should be accompanied by its physical removal from the network, otherwise the device may reappear.

To prevent the device from reappearing, you must do one of three things:

- actually disconnect the device from your network
- apply to the device a Network Property Group or Set with the property, "Allow devices" set to "Off" (**Administration** > **Network Configuration** > **Network Property Groups**)
- use the Hide command to stop a device from being rediscovered

Note: If a device has not been seen for the period set (in **Administration** > **System preferences** > **Expiry** —see *Changing the device expiry intervals* on page 193), Network Discovery automatically purges it.

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

The Deactivate, Hide, and Purge commands are available on the Network Map, through the Object menu. The commands are also available through the Device Manager Device Visibility panel.

If you want to Activate a device that you have hidden or deactivated, see *Activating devices* on page 184.

Hiding Devices

This command removes the device from the Network Map and all reports, though a complete record of the device and its history is kept. The only way to bring the device back to the Network Map is to use the Activate command. Once hidden, this device will appear on the list at **Status** > **Hidden Devices**.

The device remains hidden until reverted manually by an administrative command. For example, if you have a MAC-only device that appears on the map, and you don't want to see it, "Hiding" it is the best way to get rid of it. Hidden devices still count towards your device license limit.

To Hide a device

1. Select a device on the Network Map.
2. Click **Object** > **Visibility** > **Hide**.

   A confirmation message appears.
3. Click **OK**.

Purging Devices

If you use Purge, the device will vanish from the map and database, but will reappear if the device is still in the Network Discovery IP range. Purging removes all traces of the device from the system, including all identification and history. If the device is still on the network, it may be rediscovered at some future time.

The only way to make sure a device never reappears on the Network Map or in Network Discovery reports is to use the Hide command.

Warning: The Purge command cannot be undone.

To Purge a device

1. Select a device on the Network Map.
2. Click **Object** > **Visibility** > **Purge**.

   A confirmation message appears.
3. Click **OK**.

Deactivating Devices

This command makes a device inactive. Network Discovery will stop monitoring the device's statistics. If the device is rediscovered by Network Discovery, it will be reactivated, and will return to the Network Map. Otherwise, you can use the Activate command to manually bring this device back to the Network Map. When deactivated, this device will appear on the list at **Status** > **Deactivated Devices**.

To Deactivate a device

1. Select a device on the Network Map.
2. Click **Object** > **Visibility** > **Deactivate**.

   A confirmation message appears.
3. Click **OK**.

15 CHAPTER Using an Aggregator

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 Network Discovery version 5.1.

Topics in this chapter include:

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
- Alarms Viewer
- Events Browser

Also, with an Aggregator, you have an integrated data source for exporting onto data access applications using the Open Database Connectivity Standard (ODBC). See the *Data Export Guide* for more information.

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.

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

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.

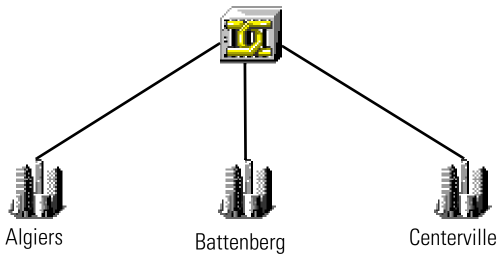
- You can use the Aggregator as a regular appliance to monitor a part of your network, as you would with any of your Peregrine appliances.
- You can use the Aggregator as a regular appliance to monitor only the backbone of your network, your important routers and servers, as well as the other Peregrine 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.

Set-up Example

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

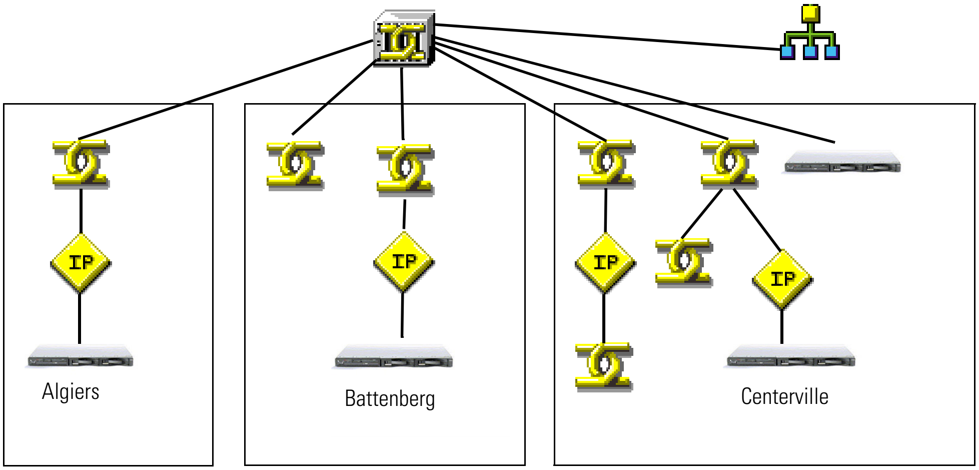
Figure 15-1: Simple conceptual network map



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

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

Figure 15-2: Network map with Peregrine appliances and routers



Tip: If the Network Map for your Aggregator does look like this, you can right-click on each Peregrine appliance to open map windows for each appliance.

Installing your Aggregator license

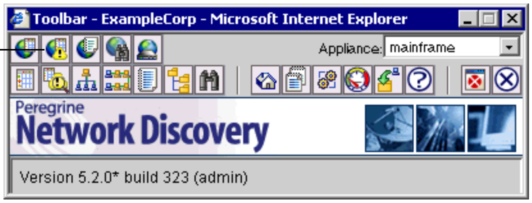
Only one Peregrine appliance on your network needs to have the Aggregator license. So, you must decide which appliance that will be. If you are not sure how to decide, contact Peregrine Systems Customer Support.

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 *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 15-3: Aggregate Toolbar



Toolbar - ExampleCorp - Microsoft Internet Explorer

Appliance: mainframe

Peregrine Network Discovery

Version 5.2.0* build 323 (admin)

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 15-1: Extra row of Aggregator buttons and their functions

Icon	Button name	Description
🌐	Aggregate Health Panel	Opens the Aggregate Health Panel.
🌐	Aggregate Alarms Viewer	Opens the Aggregate Alarms Viewer.
🌐	Aggregate Events Browser	Opens the Aggregate Events Browser.
🌐	Aggregate Find	Opens the Aggregate Find.
🌐	Remote Appliances	Opens a page showing all the remote appliances that are configured to work with the Aggregator.
Appliance: Gigabyte ▾	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 or DNS name 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 or DNS name, 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.

   Note: This can be any account on the remote appliance, as long as the account has its web access enabled, and is of the same type (Demo, IT Employee, IT Manager, or Admin), and has the same password as an account on the Aggregator.

6. Select an Aggregate health update interval.

   Note: More frequent updates use 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 211. 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. The default is "No proxy."

- no proxy
- proxy via local appliance
- proxy via local appliance and remote appliances
- proxy via remote appliance

9 Click **Change**.

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 Home Base page

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.

Important: There can be duplicate devices. The Aggregator does not eliminate duplicates. If a device has been included in discovery ranges for more than one remote appliance, you will see that device appear multiple times in an Aggregate Health Panel report.

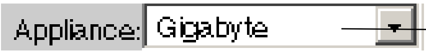
Using the pull-down list on the Toolbar

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 15-4: Remote appliance pull-down list



Appliance: Gigabyte

Remote appliance in the pull-down list (there is no asterisk (*)

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 appliances. The Toolbar buttons only work with the remote appliance selected from the pull-down list.

The difference between Home and Home Base

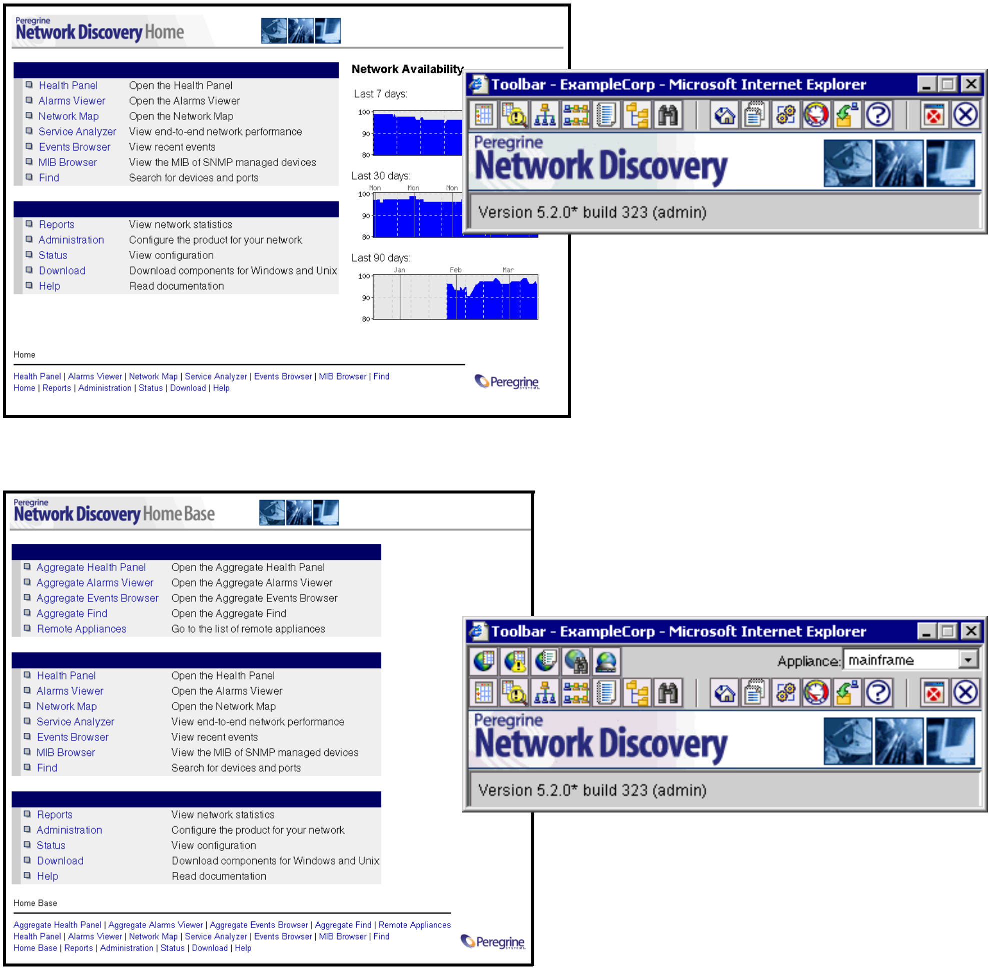
When you log into a regular Peregrine appliance, you see the Toolbar and the Home page.

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 15-5: Home and Home Base



Peregrine Network Discovery Home

Health Panel	Open the Health Panel
Alarms Viewer	Open the Alarms Viewer
Network Map	Open the Network Map
Service Analyzer	View end-to-end network performance
Events Browser	View recent events
MIB Browser	View the MIB of SNMP managed devices
Find	Search for devices and ports

Reports	View network statistics
Administration	Configure the product for your network
Status	View configuration
Download	Download components for Windows and Unix
Help	Read documentation

Network Availability

Last 7 days:

Last 30 days:

Last 90 days:

Home

Health Panel | Alarms Viewer | Network Map | Service Analyzer | Events Browser | MIB Browser | Find
Home | Reports | Administration | Status | Download | Help

Peregrine

Toolbar - ExampleCorp - Microsoft Internet Explorer

Peregrine Network Discovery

Version 5.2.0* build 323 (admin)

Peregrine Network Discovery Home Base

Aggregate Health Panel	Open the Aggregate Health Panel
Aggregate Alarms Viewer	Open the Aggregate Alarms Viewer
Aggregate Events Browser	Open the Aggregate Events Browser
Aggregate Find	Open the Aggregate Find
Remote Appliances	Go to the list of remote appliances

Health Panel	Open the Health Panel
Alarms Viewer	Open the Alarms Viewer
Network Map	Open the Network Map
Service Analyzer	View end-to-end network performance
Events Browser	View recent events
MIB Browser	View the MIB of SNMP managed devices
Find	Search for devices and ports

Reports	View network statistics
Administration	Configure the product for your network
Status	View configuration
Download	Download components for Windows and Unix
Help	Read documentation

Home Base

Aggregate Health Panel | Aggregate Alarms Viewer | Aggregate Events Browser | Aggregate Find | Remote Appliances
Health Panel | Alarms Viewer | Network Map | Service Analyzer | Events Browser | MIB Browser | Find
Home Base | Reports | Administration | Status | Download | Help

Peregrine

Toolbar - ExampleCorp - Microsoft Internet Explorer

Appliance: mainframe

Peregrine Network Discovery

Version 5.2.0* build 323 (admin)

Using the Aggregate Health Panel

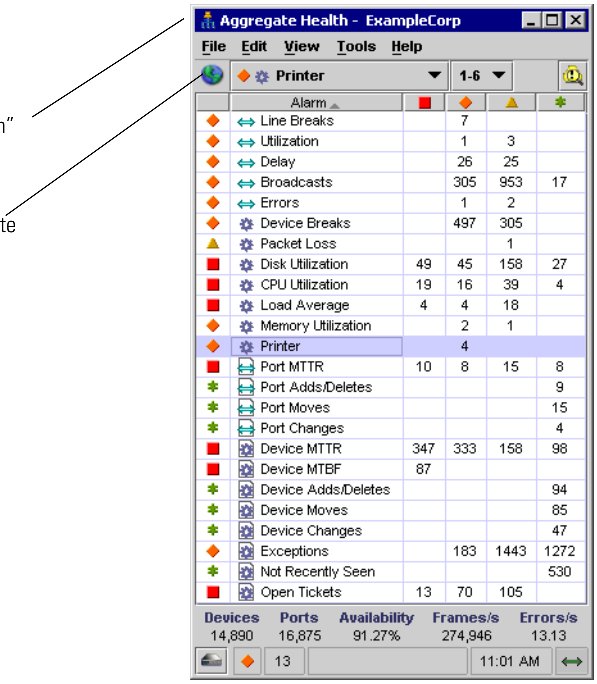
The Aggregate Health Panel looks similar to the regular Health Panel; it has all the same buttons and statistics. However, the Aggregate Health Panel combines all the statistics from all the aggregated Peregrine appliances in your network.

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 alarms 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 Aggregate 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 a network overview with the Health Panel* on page 53.

Figure 15-6: The Aggregate Health Panel



Banner says “Aggregate Health”

Globe symbol also indicates Aggregate Health Panel

	Alarm	■	◆	▲	✱
◆	Line Breaks		7		
◆	Utilization		1	3	
◆	Delay		26	25	
◆	Broadcasts		305	953	17
◆	Errors		1	2	
◆	Device Breaks		497	305	
▲	Packet Loss			1	
■	Disk Utilization	49	45	158	27
■	CPU Utilization	19	16	39	4
■	Load Average	4	4	18	
◆	Memory Utilization		2	1	
◆	Printer		4		
■	Port MTTR	10	8	15	8
✱	Port Adds/Deletes				9
✱	Port Moves				15
✱	Port Changes				4
■	Device MTTR	347	333	158	98
■	Device MTBF	87			
✱	Device Adds/Deletes				94
✱	Device Moves				85
✱	Device Changes				47
◆	Exceptions		183	1443	1272
✱	Not Recently Seen				530
■	Open Tickets	13	70	105	

Devices	Ports	Availability	Frames/s	Errors/s
14,890	16,875	91.27%	274,946	13.13

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 an address range of more than one Peregrine appliance, the device will appear more than once in the Aggregate 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 the **Appliance Health** page for that Peregrine appliance.

Note: The local Peregrine appliance is always at the top of the list with an asterisk (*).

The Aggregate Events Browser

The Aggregate Events Browser is almost identical to the regular Events Browser. The major difference is that the "Appliance" column shows which appliance is the source of the event data.

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.

The Aggregate Alarms Viewer

The Aggregate Alarms Viewer is almost identical to the regular Alarms Viewer. The major difference is that the "Appliance" column shows which appliance is the source of the alarm data.

The Aggregate Find

The Aggregate Find is almost identical to the regular Find feature. The major difference is that there are fewer find options in the Aggregate Find.

Table 15-2: Difference between Regular Find and Aggregator Find

	Regular Find	Aggregate Find
Easy Find	✓	—
Device Title	✓	✓
IP Address	✓	✓
MAC Address	✓	✓
Asset Tag	✓	✓
Domain Name	✓	✓
NetBIOS Name	✓	✓
NetBIOS Workgroup	✓	✓
Ticket	✓	—
Family	✓	✓
Model	✓	✓
Operating System	✓	✓
Network Function	✓	✓
SNMP Description	✓	✓
SNMP Contact	✓	✓
SNMP Name	✓	✓
SNMP Location	✓	✓
SNMP Serial Number	✓	✓
DNS Query	✓	—
NetBIOS Query	✓	—

Deleting Remote Appliances

If you want to delete all the data associated with this appliance, you must delete it from the list of remote appliances.

To delete a remote appliance from the Aggregator

1. On the Aggregator, click **Administration** > **Remote appliance administration** > **Delete a remote appliance.**
2. Select a remote appliance and click **Delete.**
3. A confirmation message appears.
4. Click **Delete.**

CHAPTER 16

Using Proxy Services

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:

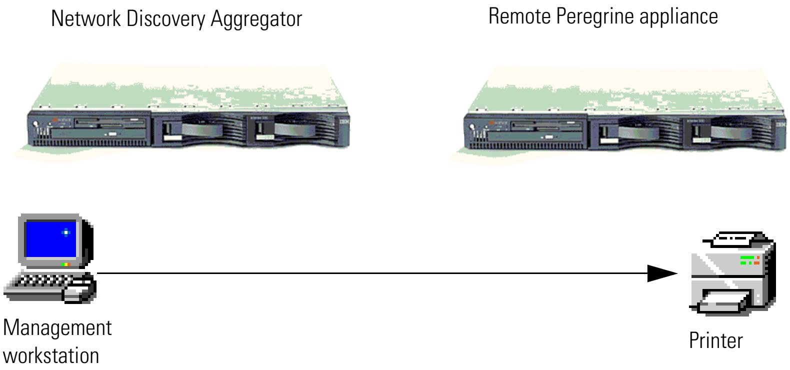
Four examples

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 16-1: 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** > **System preferences** > **Appliance proxy services.**
3. Select "Disable proxy services" (this is the default setting).
4. Click **Change.**

To set up on the Aggregator

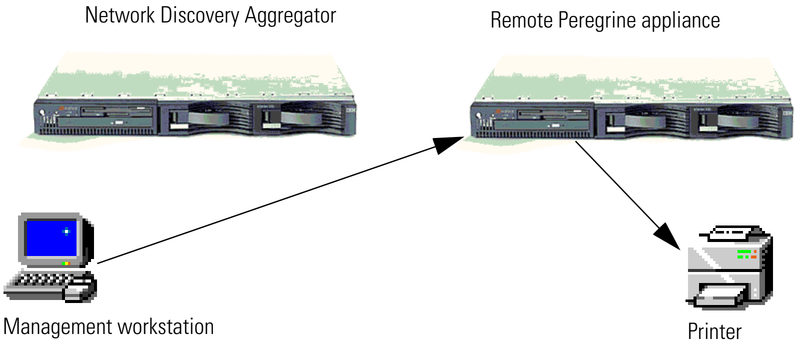
1. Log into the Aggregator Peregrine appliance.
2. Click **Administration** > **System preferences** > **Appliance proxy services.**
3. Select "Disable proxy services" (this is the default setting).
4. Click **Change.**

   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 16-2: 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** > **System preferences** > **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.

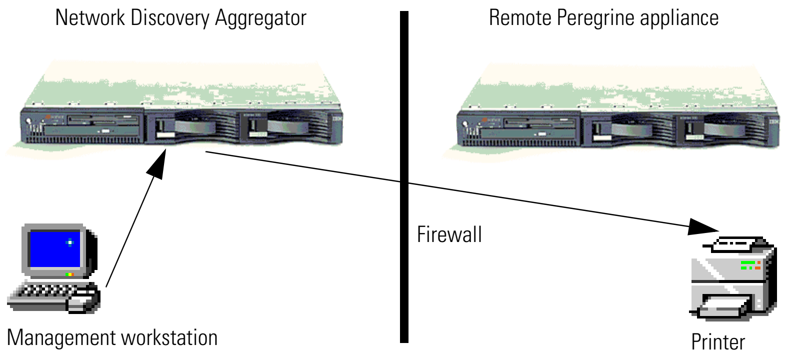
4 Click **Modify Properties.**

5 Click **proxy via remote appliance.**

6 Click **Change.**

Proxy access through the Aggregator

Figure 16-3: 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 Aggregator

1 Log into the Aggregator Peregrine appliance.

2 Click **Administration** > **System preferences** > **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.

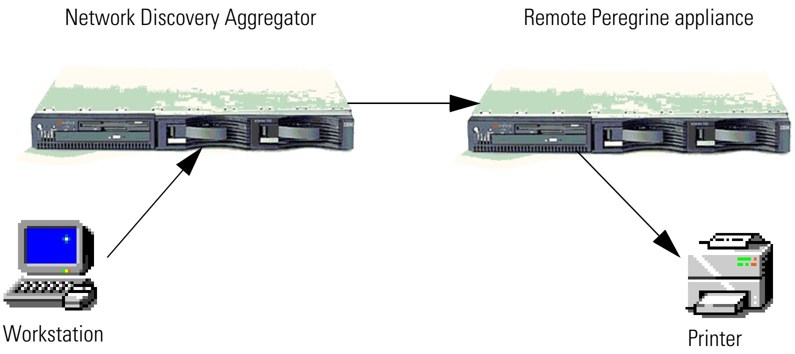
7 Click **Modify Properties.**

8 Click **proxy via local appliance.**

9 Click **Change.**

Proxy access through the Aggregator and remote appliances

Figure 16-4: 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** > **System preferences** > **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** > **System preferences** > **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.**

17 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

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

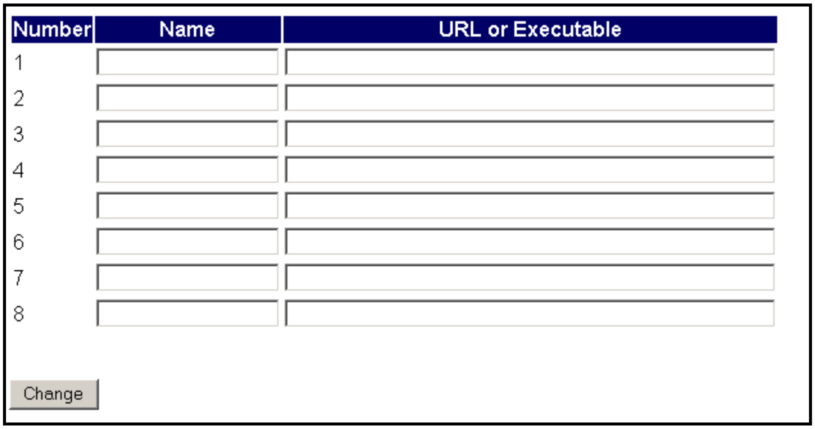
1. Click **Administration** > **System preferences** > **Element management.**

   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 17-1: Setting up the Default URL



Number	Name	URL or Executable
1		
2		
3		
4		
5		
6		
7		
8		

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** > **Manage** > [**Element Management**].

In the **Object** menu, an item appears with the name you assigned in *Setting up the default URL or application* on page 220.

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.

For more information on the “?go=” commands, see the inline help at **Help > Shortcuts.**

18 CHAPTER Using Viewer

In this chapter you will find information on the following topics:

Introduction to Viewer

This tool allows you to view the detailed information contained within a scan file (.xsf only). This provides a convenient way of displaying software, hardware and asset information collected for an individual computer. The Viewer is aimed at technical support and help desk staff who need detailed configuration analysis and diagnostics.

To use Viewer, you must make Network Discovery aware of Desktop Inventory. For more information, see *Using Network Discovery with Desktop Inventory and Desktop Administration*.

Launching Viewer

The Viewer is accessible through the Device Manager.

Note: When setting up accounts (**Administration** > **Account administration** > **Account properties**), you can configure whether the user opens the Viewer, or if they download the scan file (in **.xsf** format).

Exiting Viewer

To exit Viewer on use one of the following methods:

- Select the **Close Viewer** command from the **File** menu.
- Use the close icon ☒ in the top right of the workspace.

Viewer user interface

The Viewer workspace

The following figure shows how the Viewer workspace looks when a scan file is loaded and the **Summary** tab page is visible.

Note: The Viewer reads the xsf-based scan file from the **/scans/processed** directory on the appliance when launched. If this file is unavailable, the Viewer cannot be used to view the scan details.

The menu bar

Viewer command are accessible from the menu bar. Commands are grouped by function (‘File’, ‘Edit’, ‘View’, ‘Window’, ‘Help’). Each function has its own entry (command) in the menus. Menu commands may be activated with the mouse or the keyboard.

To open a menu:

▶ Use the mouse. Click the menu name (for example, **File**) and then click the command you want (for example, **Open Scan File...**).

Most menus invoke commands, however, some menu commands display a dialog. This is indicated by **...** after the menu command.

Toolbars

Toolbars allow you to access various commands without using the menu.

▶ Click on the toolbar icon to activate the function associated with it.

Buttons in the toolbar offer the following functionality:

Icon	Name	Function
📋	Copy	Copies the information in the currently selected tab to the clipboard.
🔍	Find File	This function finds a file within a scan.
?	Help	Displays the help text for Viewer.

Tab pages

Tab pages in Viewer allow you to examine the data from a loaded scan file. You can select the following tab pages:

- Summary
- Hardware and Configuration

- Directories and Files
- Stored Files
- Software Applications

  For the Viewer, the application data added during enrichment is displayed. This Viewer cannot perform application recognition itself.

Status bar

A status bar at the bottom of the Viewer workspace displays information on the current loaded scan file.

- The second panel displays the number of scans currently loaded
- The third panel displays the name of the currently loaded scan file along with a brief description.
- The third panel displays the progress bar showing the loading status of the Viewer.

Copying the contents of a tab page

You can save or copy the contents of the following tab pages:

- Summary
- Stored Files
- Software Applications

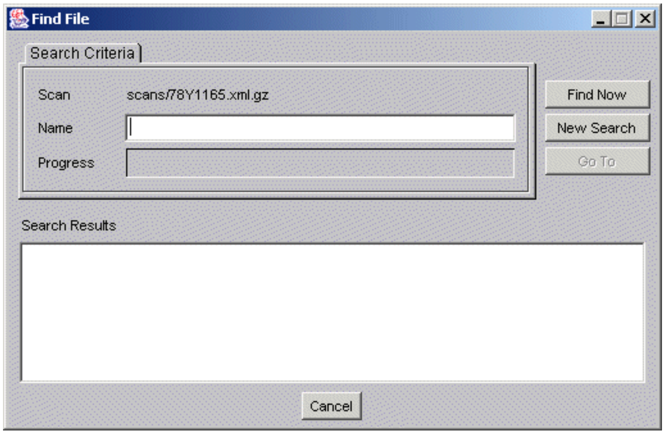
1 Click the ⎘ icon.

Searching for files within the scan

You can locate a file that exists on the scanned computer from any point within the Viewer.

To locate a file from any point:

1 Select the **Find File** command in the **Edit** menu or click the icon. The **Find File** dialog appears.



Scan scans/78Y1165.xml.gz

2 In the **Name** box type the name of the file you want to find. You can use DOS wildcard characters, (using * and ?) as well as normal alphanumeric characters.

3 Click the **Find Now** button.

If files matching the filename or mask are located, they are displayed in the **Search Results** list box.

If the search is lengthy, you can abort the search (with partial results being displayed) by clicking the **Stop** button.

4 Highlight a file entry in the **Search Results** list.

5 Click the **Goto** button or double-click on a file entry.

The **Directories and Files** tab of Viewer is displayed in the background showing the located file.

6 If you want to clear the entries and carry out a new search, click the **New Search** button.

Viewing summary data

The **Summary** tab displays a small summary of key hardware, software, user and asset information derived from the other tab pages in Viewer.

Navigation in the Viewer Summary page

To go directly to the tab page from which the summary information was derived:

- Right-click and select the option from the menu or double-click on an item.

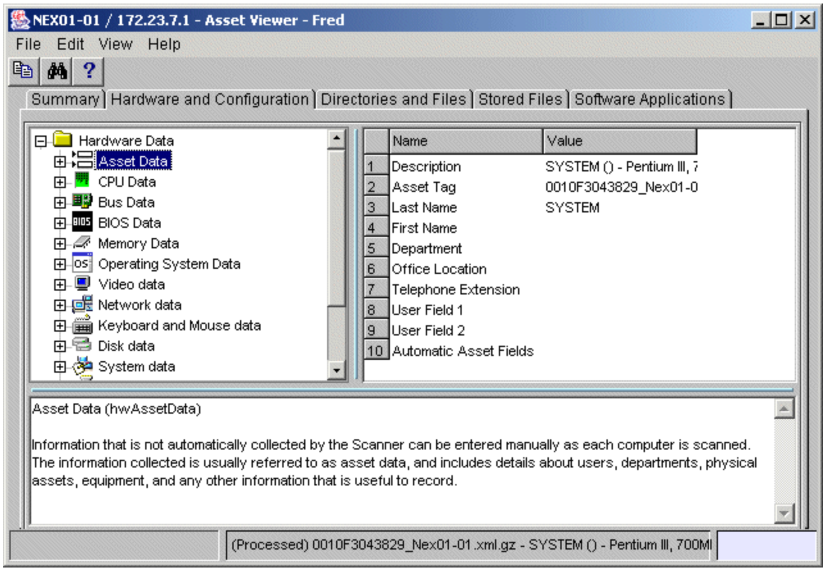
The following table shows the items on the **Summary** page, a short description and the tab page displayed when you double-click or right click on the item:

Item	Description	Page Displayed
Machine	Description field	Hardware and Configuration
CPU	CPU description	Hardware and Configuration
Memory	Memory size	Hardware and Configuration
HD Capacity	Disk size	Hardware and Configuration
OS	Operating system	Hardware and Configuration
Scan date	Date the scan file was produced	Hardware and Configuration
Scanner version	Scanner used to create the scan file	Hardware and Configuration
Scanned volumes	Drive letters scanned	Hardware and Configuration
Scanned files	Number of scanned files	Directories and Files
Stored files	Number of stored files	Stored Files
Applications	Number of applications	Software Applications

Viewing Hardware and Configuration data

The **Hardware and Configuration** tab displays:

- User and asset information collected using the asset questionnaire during the inventory.
- High level hardware information scanned during the inventory.



	Name	Value
1	Description	SYSTEM () - Pentium III, 7
2	Asset Tag	0010F3043829_Nex01-0
3	Last Name	SYSTEM
4	First Name	
5	Department	
6	Office Location	
7	Telephone Extension	
8	User Field 1	
9	User Field 2	
10	Automatic Asset Fields	

Asset Data (hwAssetData)

Information that is not automatically collected by the Scanner can be entered manually as each computer is scanned. The information collected is usually referred to as asset data, and includes details about users, departments, physical assets, equipment, and any other information that is useful to record.

(Processed) 0010F3043829_Nex01-01.xml.gz - SYSTEM () - Pentium III, 700MI

The Hardware and Configuration tab page layout

The Hardware and Configuration tab page consists of four panes. By default when you first start Viewer, only the first three are shown (**Simple** mode):

- Category tree
- Category description
- 1st level data
- 2nd level data

The following screen shot shows the **Hardware and Configuration** tab page in **Advanced** mode.

Advanced and Simple display mode

By default, when you first start the Viewer, the **Hardware and Configuration** data page is displayed in **Simple** mode.

You can display this information in a Advanced mode (hyperlinks shown and all four panes are displayed):

To switch between Advanced and Simple mode in the Hardware and Configuration data page:

▶ Select or deselect the **Advanced Hardware View** option in the **View** menu.

Category tree

The left hand side of this tab page shows a tree. This tree contains folders for each of the Asset and Hardware data items. You can click on a folder to expand it and reveal further items in the category.

The 🗂 icon indicates that multiple instances of that particular item may exist.

Category description

This pane provides a description about the data category you have selected from the tree.

2nd level data

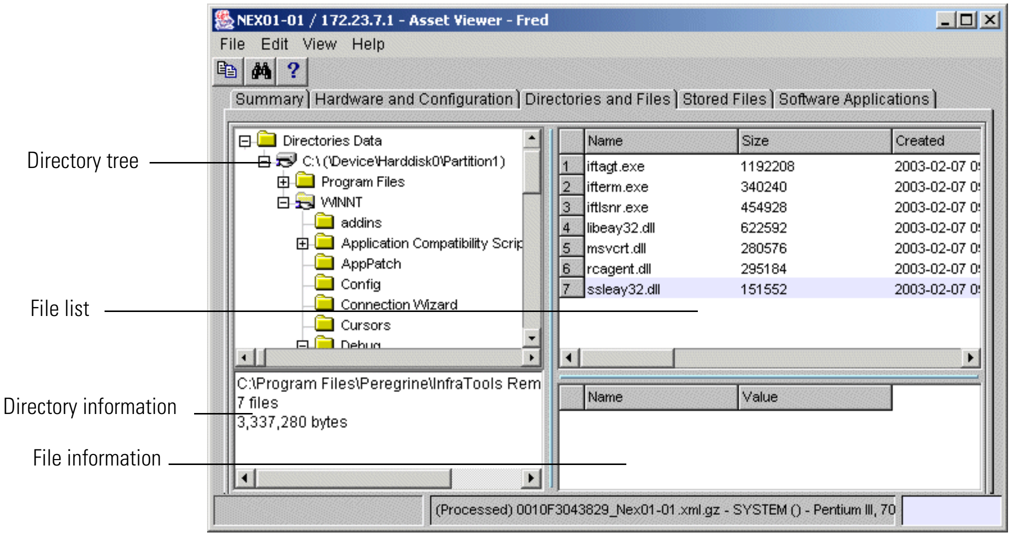
You will note that some entries in the 1st level pane may have hyperlinks. When clicked, further information for that instance of the item is show in the 2nd level data pane.

1st level data

When you have selected a category in the tree, information is shown for it in this pane.

Viewing Directories and Files data

This page is displayed by clicking the **Directories and Files** tab once you have loaded the inventory data into Viewer.



Directories Data
C:\ (\Device\Harddisk0\Partition1)
Program Files
WINNT
addins
Application Compatibility Scrip
AppPatch
Config
Connection Wizard
Cursors
Debug

	Name	Size	Created
1	iftagt.exe	1192208	2003-02-07 0
2	ifterm.exe	340240	2003-02-07 0
3	iftlsnr.exe	454928	2003-02-07 0
4	libeay32.dll	622592	2003-02-07 0
5	msvcrt.dll	280576	2003-02-07 0
6	rcagent.dll	295184	2003-02-07 0
7	ssleay32.dll	151552	2003-02-07 0

C:\Program Files\Peregrine\InfraTools Rem
7 files
3,337,280 bytes

Name	Value

(Processed) 0010F3043829_Nex01-01.xml.gz - SYSTEM () - Pentium III, 70

The **Directories and Files** tab page is split into four viewing areas (panes):

- Directory tree
- File list
- Directory information
- File information

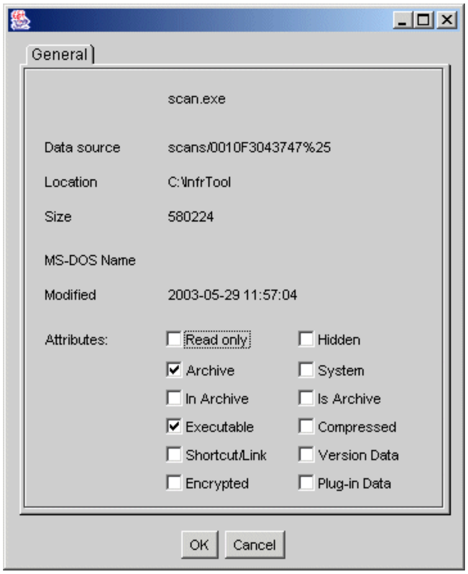
The directory tree

The directory tree is located on the left of the page. It shows the structure of the current drives displayed as a directory tree.

To obtain information about the drive or directory:

▶ Right-click on the directory and select the **Properties** option. The **Program Files Properties** dialog appears.

If the drive is a shared drive, then a **Sharing** tab is also made available.



scan.exe

Data source scans/0010F3043747%25

Location C:\InfrTool

Size 580224

MS-DOS Name

Modified 2003-05-29 11:57:04

Attributes:

□ Read only	□ Hidden
☑ Archive	□ System
□ In Archive	□ Is Archive
☑ Executable	□ Compressed
□ Shortcut/Link	□ Version Data
□ Encrypted	□ Plug-in Data

Icons used in the Viewer to denote directory status

Different icons are used to denote directory status as follows:

Icon	Directory status
📁	Indicates a shared directory.
⛔	Indicates filtered or ignored directories (as specified in the Scanner Generator). Data in the filtered directories is not stored in the scan file. This icon also represents mount points in Windows 2000 scans. Mount points are automatically filtered.

The file list

The file list is located in the top right of the page. It shows a list of files in the selected directory.

Archive files

The contents of archive files are displayed, but no signatures are shown. However, if a checksum is shown, this refers to the archive checksum.

Incremental column search

To use incremental column search to locate an entry in a column directly:

▶ Click on any row and type the word(s) or number(s) that you want to find.

The name is displayed on the status bar.

Parameters displayed for each file

The parameters displayed for each file are:

- **File Name** The name of the scanned file.
- **Size** The size of the scanned file.
- **Modified** The last modified date and time that is stored for the file in the file system.
- **Attribute** The Attribute column along with normal file attributes includes the following information:

Attribute	Meaning
r	Read only files Files that are marked read-only are protected from modification or deletion.
h	Hidden files Windows Explorer does not show hidden files by default unless you tell it to do so.
s	System files
v	Volume Label This contains no data and no more than one may exist on a disk volume (and only in the root directory).
a	If it has the archive attribute of Dos or windows The Archive attribute is used to provide an automatic record of what files have been modified since the last backup.

Attribute	Meaning
c	Compressed files These are compressed files and folders. For example, if it is a file on a compressed NTFS volume.
p	Plug-in data Whether the file data was obtained by means of a plug-in.
I	Internal file That is, if it has version data available for it. Version data (as per Windows Explorer) is displayed for all files having this attribute.
A	This file has been identified as an archive (such as a zip file).
C	This file has been identified inside an archive.
X	This file has been identified as an executable file.
D	This file has been identified as a device driver.

- **Exe/Arc**

  The Exe/Arc Type column for executable files, indicates the file type. For archive files it indicates the compression type.

- **Plug-in data**

  Indicates which files have plug-in data. Data file recognition plug-ins may store some information for the files that they recognize. This normally includes the name and the version of the program that was used to create the file and other relevant information. The Plug-in data column, displays ‘Yes’ for those files that have plug-in information. For these files, the plug-in information is displayed in the file information pane.

- **Signature**

  The signature is a number that is calculated from the first 8 Kbytes of a file. It is usually sufficient to uniquely identify a file.

Directory information

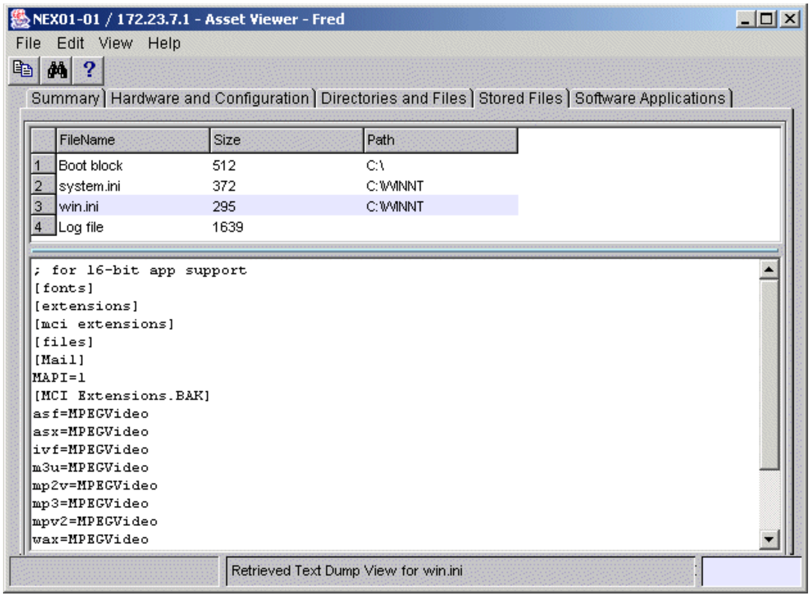
The directory information pane beneath the directory tree displays information about the selected directory. It shows the number of files in the directory and the total size of the files.

File information

Beneath the file list is the file information pane, which displays additional information for the executable files, where internal version information is included in the file header.

Viewing stored files data

This page displays the contents of key files collected during the inventory, that is, files stored in the scan file during scan time. Typically these are system configuration files, for example, **Autoexec.bat, Win.ini**.



	FileName	Size	Path
1	Boot block	512	C:\
2	system.ini	372	C:\WINNT
3	win.ini	295	C:\WINNT
4	Log file	1639	

```
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
[MCI Extensions.BAK]
asf=MPEGVideo
asx=MPEGVideo
ivf=MPEGVideo
m3u=MPEGVideo
mp2v=MPEGVideo
mp3=MPEGVideo
mpv2=MPEGVideo
wax=MPEGVideo
```

Retrieved Text Dump View for win.ini

The Stored File tab page is split into two viewing areas:

- **Stored file list** The top pane displays a list of stored files. You can sort (in ascending and descending order) the contents of a column by clicking on a column header.
- **Stored file contents** The bottom pane displays the contents of a selected stored file. Text files are displayed as text, other files are displayed in a combined HEX- and ACSII-views.

Toggling the display mode

Using the **Toggle Display mode** option it is possible to change the view from hex to text (and vice versa).

To use the Toggle Display mode option in the Viewer:

1. In the **Stored file list** (top pane), click on the file that you want to view.
2. In the bottom pane, select the **Toggle Display Mode** command from the right-click menu. The display mode switches between hex and text display.

Saving or copying the contents of a stored file

The contents of a stored file can be saved to a file for future reference or for restoring the original files if they have been lost.

Locating the directory of a stored file

To locate the directory of a displayed file (this will be displayed on the Software page):

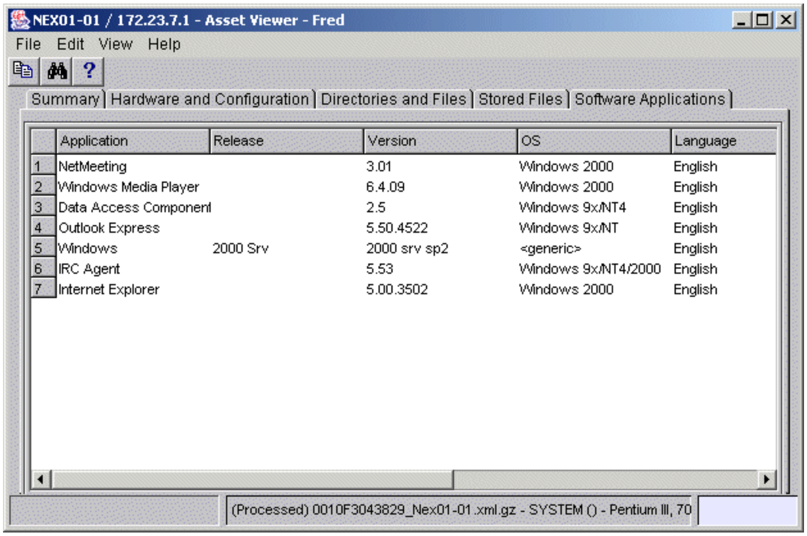
▶ Right-click anywhere in the top pane and select the **Go to Directory** command from the shortcut menu, or double-click on the file.

The software page is displayed, with the file highlighted.

Note: This will only work if the directory/file is available.

Viewing software application data

The **Software Applications** tab displays applications that have been recognized during the enrichment process. See *Using Network Discovery with Desktop Inventory and Desktop Administration*.



	Application	Release	Version	OS	Language
1	NetMeeting		3.01	Windows 2000	English
2	Windows Media Player		6.4.09	Windows 2000	English
3	Data Access Component		2.5	Windows 9x/NT4	English
4	Outlook Express		5.50.4522	Windows 9x/NT	English
5	Windows	2000 Srv	2000 srv sp2	<generic>	English
6	IRC Agent		5.53	Windows 9x/NT4/2000	English
7	Internet Explorer		5.00.3502	Windows 2000	English

(Processed) 0010F3043829_Nex01-01.xml.gz - SYSTEM () - Pentium III, 70

It displays application name, release, version, operating system, language, publisher information and the path to the file recognized as the **Main** file. Main files for an application (for example, Winword.exe) identify the application.

Double clicking on an application in the list or right-clicking on an entry and selecting the **Goto** command will display the **Directories and Files** tab with the application highlighted. The **Directories and Files** tab shows the file/ directory identifying the application.

The following additional command is also available by right-clicking on an application entry.

- **Copy** Copies the contents of the Applications tab page to a text format and places it on the clipboard. You can paste the contents to an editor of your choice.

19 CHAPTER

Working with SNMP Traps

Peregrine Network Discovery determines network events and places them in an internal events database. Typically an operator can browse these events within the Events Browser, but there are circumstances where the events would be exported to a third party system. Peregrine Network Discovery may export SNMP V2C trap event notifications.

To see the full contents of the PeregrineTrapMIB.txt file, see the Network Discovery Download directory.

Network Discovery Notifications

Peregrine Network Discovery issues traps using SNMPv2c messages. SNMPv2c notifications are the successor to SNMP V1 traps. An SNMPv2c notification can contain several objects, which are then parsed by the collector to interpret the event contents. The interpreted contents are then written to a database or forwarded to the notification engine of another NMS system.

There are two notifications, *deviceEvent* and *portEvent*. Each carries a set of SNMP OIDs. These variables cannot be retrieved by an SNMP get request. They are only available as SNMPv2c notification messages.

deviceEvent Notification

The deviceEvent notification is sent for events that correspond to a device, rather than a line. For a detailed description of events that correspond to a device versus those that correspond to a line, see the Network Discovery reference manual.

The deviceEvent event (OID: .1.3.6.1.4.1.1467.100.100.2.1) contains the following members:

Order	Object	Type	Description
1	serverID .1.3.6.1.4.1.1467.100.100.1.1	Integer	ServerID is an integer that has been configured by the administrator of the Peregrine Network Discovery server; it is 1 by default. The ServerID makes it easier for consumers of the inventory to correlate devices managed by different Peregrine Network Discovery servers.
2	eventID .1.3.6.1.4.1.1467.100.100.1.2.1	Unsigned 32	Increasing sequence number associated with this event. This object is present for compatibility only. It is always blank.
3	datetime .1.3.6.1.4.1.1467.100.100.1.2.2	Octet String	Date and time when event occurred (YYYYMMDD HH:MM:SS).
4	category 1.3.6.1.4.1.1467.100.100.1.2.3	Integer	Category of the event: Errors In, Collisions, Errors Out, Load Average, CPU, Memory, Virtual Memory, Disk, Discard Eligibility In, Discard Eligibility Out, FECN, BECN, Utilization In, Utilization Out, PacketLoss, Data Delivery Ratio, Frame Delivery Ratio, Delay, Line Utilization, Breaks, Backplane Utilization, Source of Broadcasts, Paper Count, UPS Battery Capacity, UPS Battery Time Remaining, Add, Delete, ConnectionChange, PropertyChange.

Order	Object	Type	Description
5	state .1.3.6.1.4.1.1467.100.100.1.2.4	Integer	Alarm state of the event: info (Add, Delete, PropertyChange,ConnectionChange) na-ok, na-info, na-minor, na-major, na-critical, ok-na, ok-info, ok-minor, ok-major, ok-critical, info-na, info-ok, info-minor, info-major, info-critical, minor-na, minor-ok, minor-info, minor-major, minor-critical, major-na, major-ok, major-info, major-minor, major-critical, critical-na, critical-ok, critical-info, critical-minor, critical-major.
6	deviceNMID .1.3.6.1.4.1.1467.100.100.1.2.5.1	Unsigned 32	Network Manager Identification
7	deviceType .1.3.6.1.4.1.1467.100.100.1.2.5.2	Unsigned 32	The device type (Icon).
8	deviceTag .1.3.6.1.4.1.1467.100.100.1.2.5.3	Octet String	The name of the device.
9	macAddress .1.3.6.1.4.1.1467.100.100.1.2.5.4	Physical Address	The MAC address associated with the device.
10	ipv4Address .1.3.6.1.4.1.1467.100.100.1.2.5.5	IP Address	The IPv4 address associated with the device (if any).
11	deviceTitle .1.3.6.1.4.1.1467.100.100.1.2.5.6	Octet String	The (network map) title of the device as defined by the appliance administrator.
12	priority .1.3.6.1.4.1.1467.100.100.1.2.5.7	Integer	The priority of the device as defined by the appliance administrator: 1, 2, 3, 4, 5 or 6.
13	direction .1.3.6.1.4.1.1467.100.100.1.2.7	Integer	Direction of port that triggered event: notAvailable, in, out.
14	value .1.3.6.1.4.1.1467.100.100.1.2.8	Octet String	Value of threshold variable that triggered event. Value is not present where it makes no sense, for e.g. categories break, add, or delete.
15	units .1.3.6.1.4.1.1467.100.100.1.2.9	Integer	The unit of the Value. Units always appear whenever Value does. Can be one of: notAvailable, count, day, persec, percent, hour, unknown.

portEvent Notification

The *portEvent* notification is sent for events that correspond to a port or line, rather than a device. For a detailed description of events that correspond to a device versus those that correspond to a device, see the Network Discovery reference manual.

The portEvent event (OID: .1.3.6.1.4.1.1467.100.100.2.2) contains the following members:

Order	Object	Type	Description
1	serverID .1.3.6.1.4.1.1467.100.100.1.1	Integer	ServerID is an integer that has been configured by the administrator of the Peregrine Network Discovery server; it is 1 by default. The ServerID makes it easier for consumers of the inventory to correlate devices managed by different Peregrine Network Discovery servers.
2	eventID .1.3.6.1.4.1.1467.100.100.1.2.1	Unsigned 32	Increasing sequence number associated with this event. This object is present for compatibility only. It is always blank.
3	datetime .1.3.6.1.4.1.1467.100.100.1.2.2	Octet String	Date and time when event occurred (YYYYMMDD HH:MM:SS).
4	category .1.3.6.1.4.1.1467.100.100.1.2.3	Integer	Category of the event: Errors In, Collisions, Errors Out, Load Average, CPU, Memory, Virtual Memory, Disk, Discard Eligibility In, Discard Eligibility Out, FECN, BECN, Utilization In, Utilization Out, PacketLoss, Data Delivery Ratio, Frame Delivery Ratio, Delay, Line Utilization, Breaks, Backplane Utilization, Source of Broadcasts, Paper Count, UPS Battery Capacity, UPS Battery Time Remaining, Add, Delete, ConnectionChange, PropertyChange.
5	state .1.3.6.1.4.1.1467.100.100.1.2.4	Integer	Alarm state of the event: info (Add, Delete, PropertyChange,ConnectionChange) na-ok, na-info, na-minor, na-major, na-critical, ok-na, ok-info, ok-minor, ok-major, ok-critical, info-na, info-ok, info-minor, info-major, info-critical, minor-na, minor-ok, minor-info, minor-major, minor-critical, major-na, major-ok, major-info, major-minor, major-critical, critical-na, critical-ok, critical-info, critical-minor, critical-major.

6	deviceNMID .1.3.6.1.4.1.1467.100.100.1.2.5.1	Unsigned 32	Network Manager Identification
7	deviceType .1.3.6.1.4.1.1467.100.100.1.2.5.2	Unsigned 32	The device type (Icon).
8	deviceTag .1.3.6.1.4.1.1467.100.100.1.2.5.3	Octet String	The name of the device.
9	macAddress .1.3.6.1.4.1.1467.100.100.1.2.5.4	Physical Address	The MAC address associated with the device.
10	ipv4Address .1.3.6.1.4.1.1467.100.100.1.2.5.5	IP Address	The IPv4 address associated with the device (if any).
11	deviceTitle .1.3.6.1.4.1.1467.100.100.1.2.5.6	Octet String	The (network map) title of the device as defined by the appliance administrator.
12	priority .1.3.6.1.4.1.1467.100.100.1.2.5.7	Integer	The priority of the device as defined by the appliance administrator: 1, 2, 3, 4, 5 or 6.
13	portNMID .1.3.6.1.4.1.1467.100.100.1.2.6.1	Unsigned 32	Network Manager Identification.
14	portIndex .1.3.6.1.4.1.1467.100.100.1.2.6.2	Octet String	An index value that uniquely identifies this port within a module. The value is determined by the location of the port on the module. Valid entries are 1 to the value of moduleNumPorts for this module.
15	ifSpeed .1.3.6.1.4.1.1467.100.100.1.2.6.3	Integer (Counter 64)	An estimate of the interface's current bandwidth in bits per second. For interfaces, which do not vary in bandwidth, or for those where no accurate estimation can be made, this object should contain the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reportable by this object then this object should report its maximum value (4,294,967,295) and ifHighSpeed must be used to report the interface’s speed. For a sub-layer, which has no concept of bandwidth, this object should be zero.
16	ifType .1.3.6.1.4.1.1467.100.100.1.2.6.4	IANAifType (Integer)	The type of interface. The Internet Assigned Numbers Authority (IANA), through updating the syntax of the IANAifType textual convention, assigns additional values for ifType.
17	duplex .1.3.6.1.4.1.1467.100.100.1.2.6.5	Integer	The duplex of port within the device: full, half, or non-applicable.
18	connectedToDevice .1.3.6.1.4.1.1467.100.100.1.2.6.6	Unsigned 32	The NMID of the remote device this port connects to.

19	connectedToPort .1.3.6.1.4.1.1467.100.100.1.2.6.7	Unsigned 32	The NMID of the port on the remote device this port connects to.
20	alarmType .1.3.6.1.4.1.1467.100.100.1.2.6.8	Unsigned 32	The alarm type for this port.
21	direction .1.3.6.1.4.1.1467.100.100.1.2.7	Integer	Direction of port that triggered event: notAvailable, in, out.
22	value .1.3.6.1.4.1.1467.100.100.1.2.8	Octet String	Value of threshold variable that triggered event. Value is not present where it makes no sense, for e.g. categories break, add, or delete.
23	units .1.3.6.1.4.1.1467.100.100.1.2.9	Integer	The unit of the Value. Units always appear whenever Value does. Can be one of: notAvailable, count, day, persec, percent, hour, unknown.

Index

Peregrine
SYSTEMS®

July 23, 2004