Peregrine **Network Discovery**

User Guide

Version 5.1

Peregrine
S Y S T E M S.

Contents

1 Welcome to Peregrine's Network Discovery

CHAPTER

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).

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 license.
- Clear the database
- Receive an extension 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 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
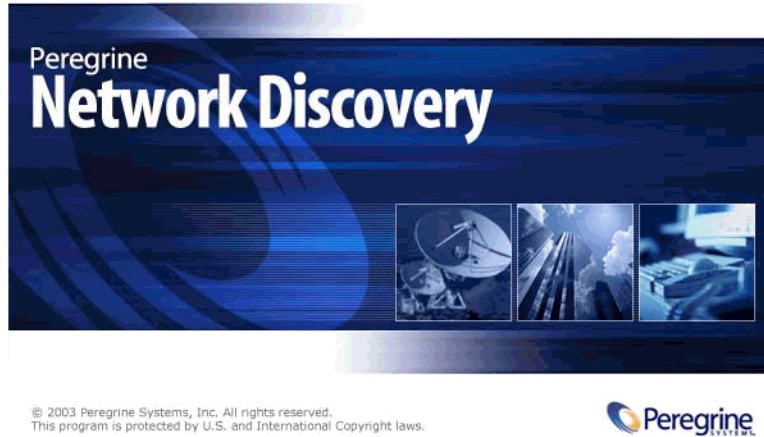
Figure 1-2: Network Discovery login window
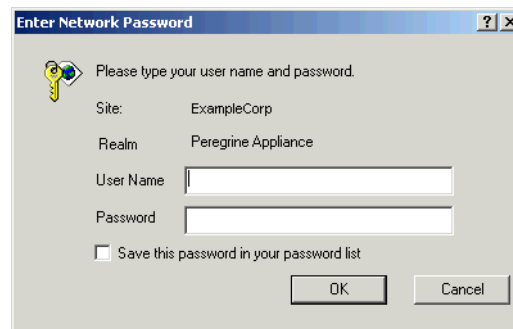
3 Enter your account name (user name) and password.

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

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

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

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

Figure 1-3: Network Discovery Toolbar
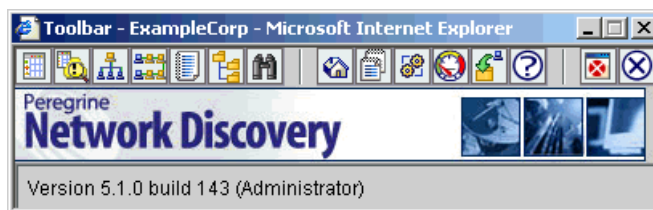
Shutdown and restart

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

Shutting down the Peregrine appliance

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

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**.
3 When the text "The system is halted" appears on the screen, power off the Peregrine 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 8–9 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* on page 18
- *Demo accounts* on page 19
- *IT Employee accounts* on page 19
- *IT Manager accounts* on page 20
- *Administrator accounts* on page 20

About accounts

There are four types of account:

- Demo
- IT Employee
- IT Manager
- Administrator

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

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

To check how many people are using a map:

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

Demo accounts

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

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

A Demo account can:

- View the Network Map, with the restriction that each map session will begin with a configuration named "Copy of Prime." The Prime configuration is maintained by an Administrator or IT Manager account.
- Change the name of devices as they appear on the Network Map
- 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
- See a device's read and write community strings (if known) in the Device Manager Configuration panel
- Purge a device, port or attribute from the Network Map
- Change device system properties
- 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

Table 2-2: What the accounts can do

	Demo	IT Employee	IT Manager	Administrator
Network Map				
Initial map configuration file	Copy of Prime	Copy of Prime	Copy of Prime	Copy of Prime
Default map configuration file	Copy of Prime	last saved or used	last saved or used	last saved or used
Open any saved map configuration	YES	YES	YES	YES
Save any number of map configurations	YES	YES	YES	YES
Save a map configuration as Prime	—	—	YES	YES
Change a device icon—user property	—	—	YES	YES
Change a device icon—system property	—	—	YES	YES
Change a package icon	YES	YES	YES	YES
Change a device's priority—user property	YES	YES	YES	YES
Change a device's priority—system property	—	—	YES	YES
Change a device's priority—user property	YES	YES	YES	YES
Change a device's priority—system property	—	—	YES	YES
Alarm Thresholds	view	view	view + change	view + change
Purge a device	—	—	YES	YES
Disconnect other accounts' map sessions	—	—	—	YES
Managers (for example, Device Manager)				

	Demo	IT Employee	IT Manager	Administrator
View read and write community strings for device	—	—	YES	YES
View and use *set* link to MIB Browser	—	—	YES	YES
SNMP query default string	"public"	"public"	from Network Discovery	from Network Discovery
Update Model	—	—	YES	YES
Configure connections	—	—	YES	YES
Break and force connections	—	—	YES	YES
MIB Browser				
Set SNMP variables	—	—	YES	YES
Read community string	view	view + edit	view + edit	view + edit
Write community string	—	—	view + edit	view + edit
Status				
View read and write community strings for network	—	—	YES	YES
Administration				
Change own password	—	YES	YES	YES
Configure own account	—	YES	YES	YES
Configure other accounts	—	—	—	YES
Manage own map configurations	—	YES	YES	YES
Copy map configurations from other accounts	—	YES	YES	YES
Select pager service provider	—	YES	YES	YES
Configure pager service provider	—	—	—	YES
Configure event filters	—	—	—	YES
Configure Peregrine appliance	—	—	—	YES
Configure network operations	—	—	—	YES
Access to shared directory	read	read	read	read/write

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 3–20 characters long. Acceptable characters are:

■ a through z (must be lower case)

■ 0 through 9

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

To add an account

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

Enter a login name. Acceptable characters are:

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

2 Click **Add Account**.

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

Figure 3-2: Add an account

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

Table 3-1: Account properties that Administrator accounts control

Property	Explanation
Account type	Determines the account's level of access to Network Discovery.
Account capabilities:	Determines what capabilities of Network Discovery the account can access
■ 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 to install updates and new licenses.
Password expiry	The number of days an account can be inactive before the password expires.
Name	The name of the account owner.
Allow others to copy map configurations	Determines whether or not other users can copy map configuration files from this account.
Append IP Address to device titles?	Determines if device titles are followed by device IP addresses (when available).
Make URLs visible	Determines if hyperlinks are followed by the associated URL (for easy cut and paste).
Draw borders on tables in text mode	If you use the "as text" button, tables will have borders. Tables are easier to read with borders, but they take 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.

Property	Explanation
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.
Default Device Manager panel	Determines which panel will appear when you open a Device Manager session.
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 panel will appear when you open a Ports session from the Device Manager. ■ Determines how many rows of data the Ports panel displays at a time. Default: 24

To select an account for customizing

1 Click **Administration** > **Account administration** > **Account properties**.

2 Select an account from the list box.

3 Click **Modify Properties**.

To modify an account

1 Select an account type from the list box.

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

2 Determine what capabilities the account will have.

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

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

4 Assign the appropriate properties.

5 Click **Modify Properties**.

Figure 3-3: Modify account properties

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 127.

Figure 3-4: Modify contact data

Modifying an account password

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

Passwords can be up to 20 characters long (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**.
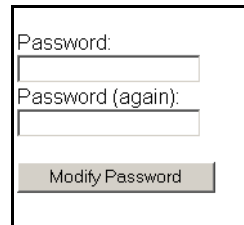
To select an account

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**.

Figure 3-5: Modify password

Deleting an account

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

Note: The account you are using to delete accounts, or the "active" account, cannot be deleted.
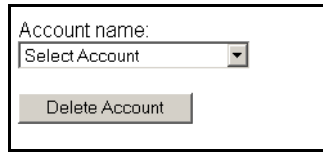
To select an account

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

2 Select an account from the list box.

3 Click **Delete Account**.

To delete an account

▶ Click **Confirm**.

Figure 3-6: Delete an account

```
Account name:
Select Account    ▼

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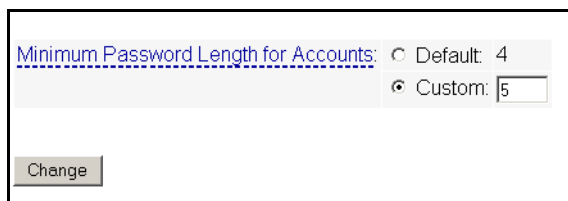
Your company may have a standard password length for all accounts in the organization. That standard may be different than the default password length in Network Discovery (which is 4-10 characters).

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 3-7: Minimum password length

CHAPTER

4 Maintaining Your Account

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: Many of these properties will be of more interest to you when you are more experienced with Network Discovery.

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

Property	Explanation
Name	The name of the account owner.
Allow others to copy map configurations	Determines whether or not other users can copy map configuration files from this account.
Append IP Address to device titles?	Determines if device titles are followed by device IP addresses (when available).
Make URLs visible	Determines if hyperlinks are followed by the associated URL (for easy cut and paste).
Draw borders on tables in text mode	If you use the "as text" button, tables will have borders. Tables are easier to read with borders, but they take more space on your screen.
Alternate colors in table rows	Tables are easier to read with alternating colors, but they take up more space on your screen.
Highlight table rows on mouse over	Lets you highlight a row you want to look at.
Show navigation bar	Determines whether or not you see the navigation hyperlinks at the bottom of pages. The hyperlinks are the same as the buttons on the Toolbar.
Time before marking statistic as stale	Applies to Device Manager, Port Manager, Line Manager, Attribute Manager, 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.

Property	Explanation
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 see a link called "Full Help". Clicking that link opens an Assistant window that displays the Full Help.
Default Device Manager panel	Determines which panel will appear when you open a Device Manager session.
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	Determines which panel will appear when you open a Device Manager Ports panel:

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 127.

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.

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
- a server administrator e-mail address has not been specified for use with Network Discovery
- the Network Discovery mail server is not working
- the receiving mail server is not working

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

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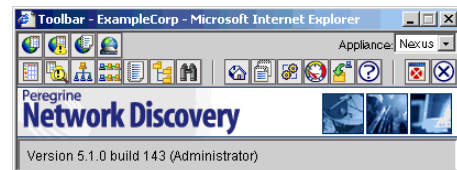
The principal difference is that the Aggregator Toolbar allows you to examine all Peregrine appliances—the Aggregator appliance and all remote appliances—without logging in to each appliance separately.

For more information on the Network Discovery Aggregator, see *Chapter 16, 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.
	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 and UNIX.
	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

individual appliance

Home

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

Aggregator appliance

extra row of hyperlinks

Home Base

Aggregate Health Panel | Aggregate Alarms Viewer | Aggregate Events Browser | 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 16, 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 a fault 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, faults, and statistics that Network Discovery has gathered about your network.

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

Alarm	■	◆	▲	✱
◆ ⟷ Line Breaks		1		
◆ ⟷ Utilization		2		
◆ ⟷ Delay		2		
– ⟷ Collisions				
▲ ⟷ Broadcasts			347	
– ⟷ Errors				
– ⟷ Frame Relay				
◆ ✿ Device Breaks		49	8	
– ✿ Packet Loss				
■ ✿ Disk Utilization	2	10	107	30
■ ✿ CPU Utilization	1		1	1
▲ ✿ Load Average			8	
– ✿ Memory Utilization				
– ✿ Backplane Utilization				
– ✿ Printer				
– ✿ UPS				
■ ⟷ Port MTTR	14	4	4	18
– ⟷ Port MTBF				
– ⟷ Port Adds/Deletes				
– ⟷ Port Moves				
✱ ⟷ Port Property Changes				9
■ ✿ Device MTTR	216	53	268	47
■ ✿ Device MTBF	35			
✱ ✿ Device Adds/Deletes				2
– ✿ Device Moves				
– ✿ Device Property Changes				
◆ ✿ Exceptions		29	12	205
– ✿ Not Recently Seen				
– ✿ Open Tickets				

Devices	Ports	Availability	Frames/s	Errors/s
5,527	2,953	100%	23,690	4.81

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

The Health Panel will show you how many alarms are on your network. You can drill down with the Alarms Viewer to see exactly what 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 194.

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

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
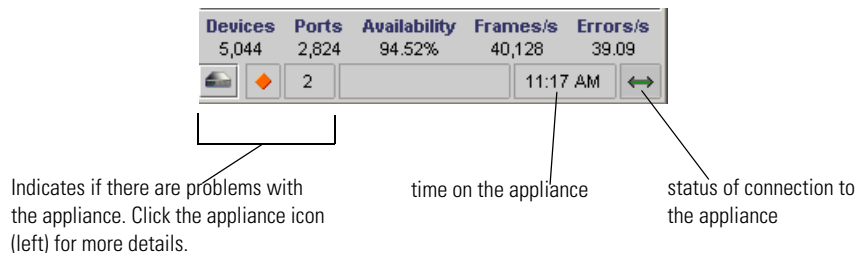
Statistic	Explanation
Devices	The number of objects in the network.
Ports	The number of ports in your network
Availability	This number represents the number of real devices with priority 3 (or higher) that are operational as a percentage of the total number of real devices with priority 3 (or higher).
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**   Result with **View** > **My User Alarms Only**
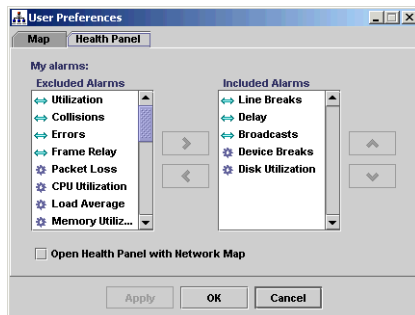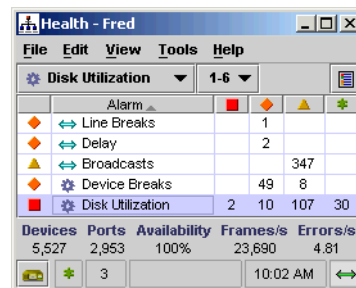
Using the Alarms Viewer

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

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.

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 5-7: Network Map
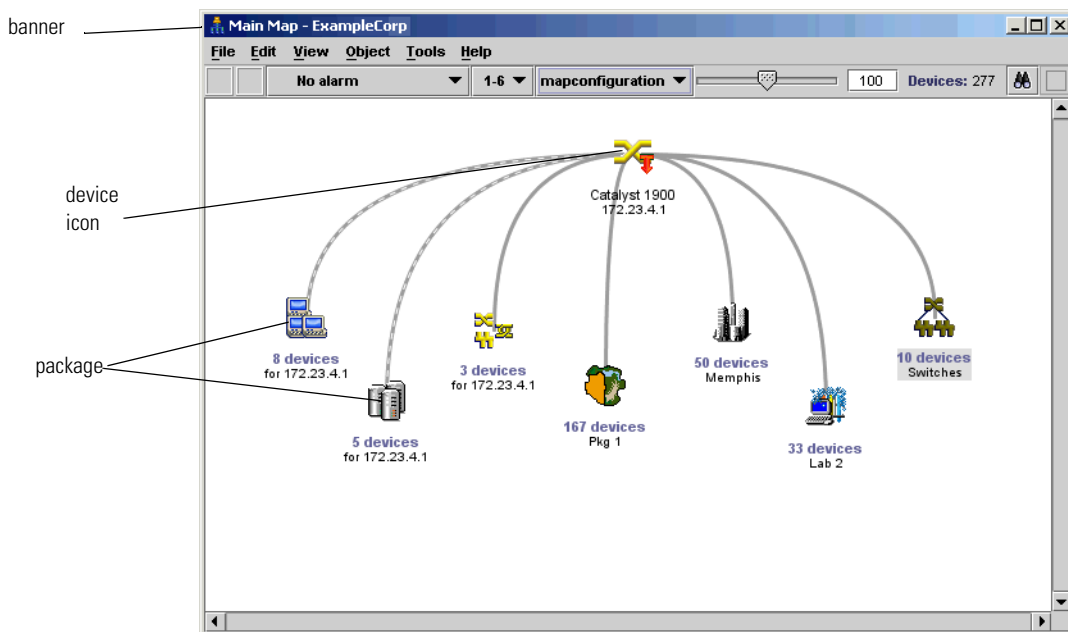
To determine what the Map will display, select a fault category on the Health Panel or by clicking the alarm list on the map status bar.

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 yellow 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 the priority of a device* on page 93.)

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 5-8: Network Map Status bar

| package alarm state | object alarm state | alarm type pull-down list | priority range pull-down list | map configuration file | map scale slider | map scale percentage in this window | number of devices in this package | Find a device by name | go up one level |
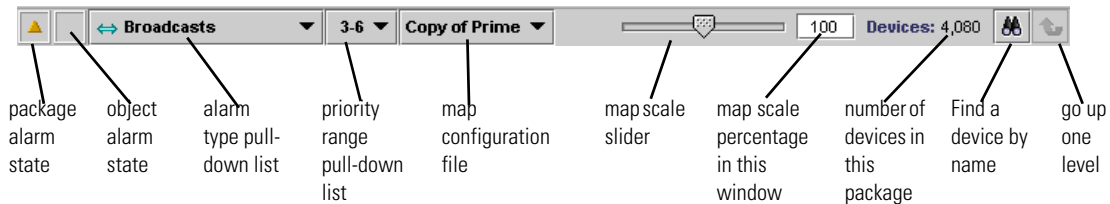
What are the icons on the map?

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	Object 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 5-9: 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
- port index identifies the port of the parent device; appears only for icons within an automatic package

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
- no port index

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)
- no port index

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.

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

By default, priorities 5 and 6 are reserved for the user. By default, priority 6 is reserved for those devices that should trigger event notification—see *Setting up Event Filters* on page 137.

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 98.

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.	2 devices for 172.23.4.4
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 107.	5040 devices Virtual Network

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 (yellow) 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 ■ an alarm has been selected but that type of alarm does not apply to this device 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 as a gray icon, 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 (**Up a Level**, **Promote**), or has had its package removed (**Unpackage**). Network Discovery does create some automatic packages. They are created during discovery and whenever you use the **Pack** or the **Unpack All** commands. For more information on packaging, see *Packaging Your Network* on page 107.
	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.
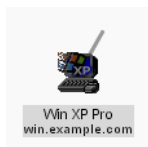
Access to the Network Map

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 and changes to the network and its objects are no longer displayed. You can change the display of open map windows but not the contents (such as packaging).

Table 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 **Disconnect** 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).
- The map is returned to the present and the Forecast dialog box is closed.

Checking the Network Forecast

This command 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.

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

While using the **Forecast** command:

- the alarm pull-down list has a green background
- 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.

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

CHAPTER

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

Topics in this chapter include:

The Device Manager

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.

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 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 Line Manager with multiple lines, it appears as shown in Figure 6-1.

To open a single Line Manager, click on one of the arrows in the middle of the screen. If an alarm has been selected, the column of arrows will display the state of that alarm on the lines. For example, if on the Health Panel, you have selected "Delay," then the column of arrows will have the title "Delay." If no type of alarm has been selected, that column will be called "Line."

You can use the hyperlinks on the 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: Click an arrow on the Multiple Line Manager to open a single Line Manager for that line
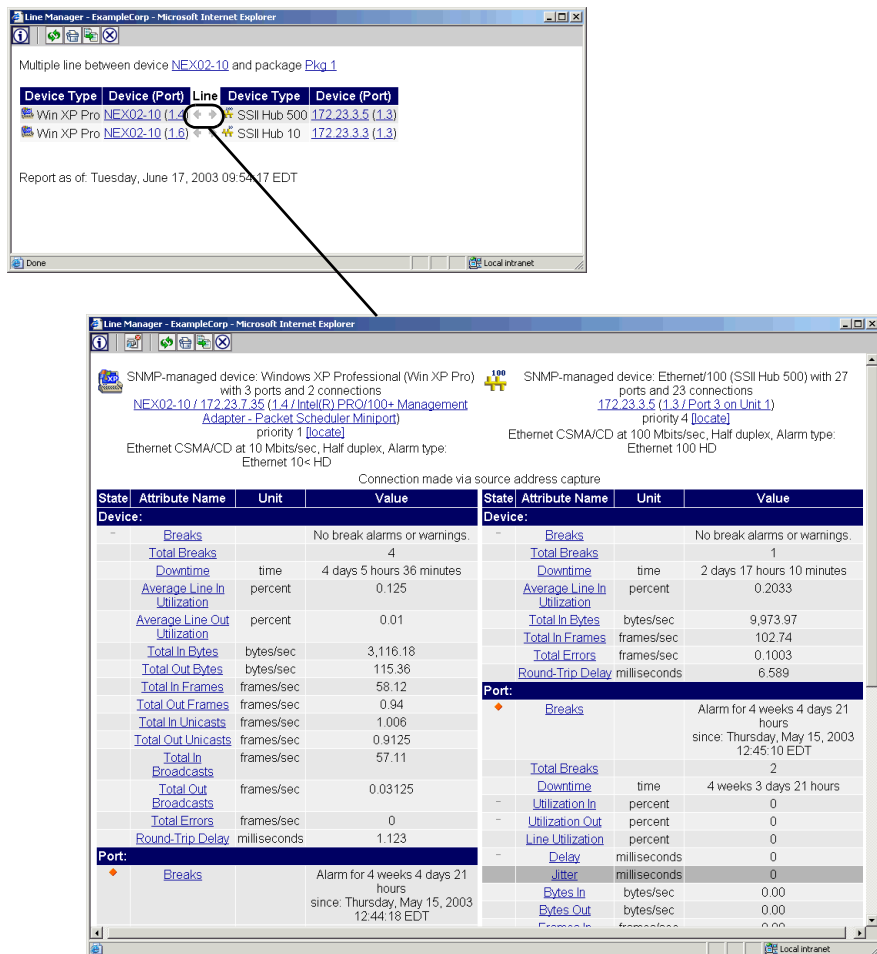
The Events Browser

Network Discovery logs events in your network. An 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 property through Network Discovery (with the Device Properties dialog)

The categories of events correspond to the alarm categories on the Health Panel.

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).

To access the Events Browser:

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

   OR

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

   OR

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

   OR

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

Figure 6-2: Events Browser

Event Entry

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

Table 6-1: Data in Events Browser table

Data	Limits/Options	Notes
Time	—	The time the event was generated.
Device Priority	1–6	—
Device type	see **Help** > **Classifications** > **Device types**	small device icon
Device (Port)	—	■ device title[a] ■ port (in parentheses)
State	Info, Minor, Major, Critical	alarm icon
Device Attribute	For a full list, see the *Reference Manual.*	—
Value	—	For more information on the attributes, see the *Reference Manual.*

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.

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 6-3: Events Browser toolbar
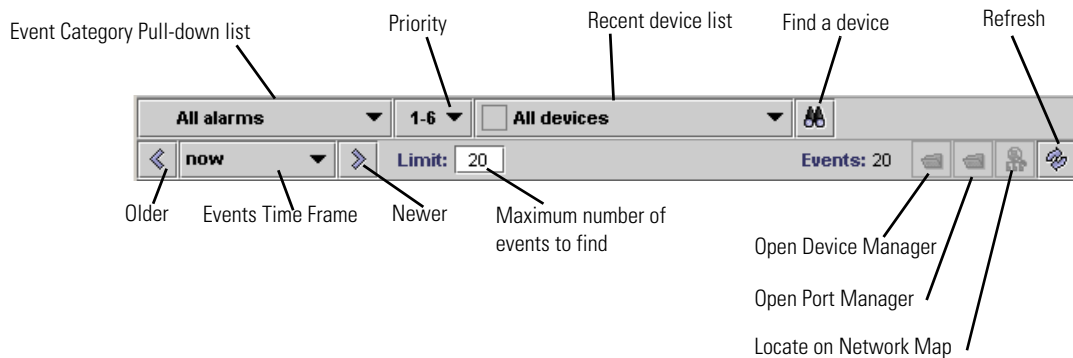
Event Category Pull-down List

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.

Limits 1-6, 2-6, 3-6, 4-6, 5-6, 6

Default 1-6

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.

Figure 6-4: Service Analyzer window (blank)
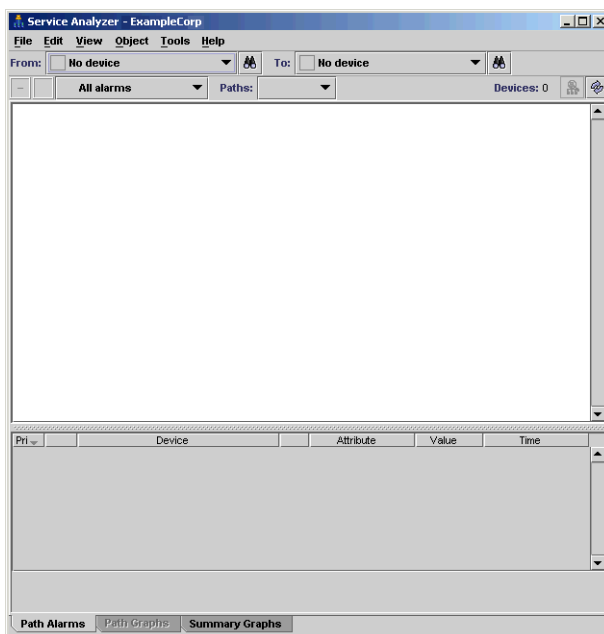
The query

The toolbar contains two search boxes: From and To. Each box searches for a device based on its name, title, or address.

Limits
- The device must be on the Network Map.

■ *Input:* "localhost" | "nmc" | MAC address | IPv4 address | IPv6 address | domain name | system-assigned title | user-assigned title | asset tag | NetBIOS name

Procedural alerts

■ To find the Peregrine appliance, enter "nmc" or "localhost".

■ To find multiple devices in the Network Discovery database, enter the first few letters of a title or the first number of an address. You are provided with a list box for each device that returned a multiple result. This allows you to select the desired device and proceed with the analysis.

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

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.

Table 6-2: Service Analyzer toolbar

Click the "Find" icons, and the Find dialog appears.

Enter the devices you want to locate.
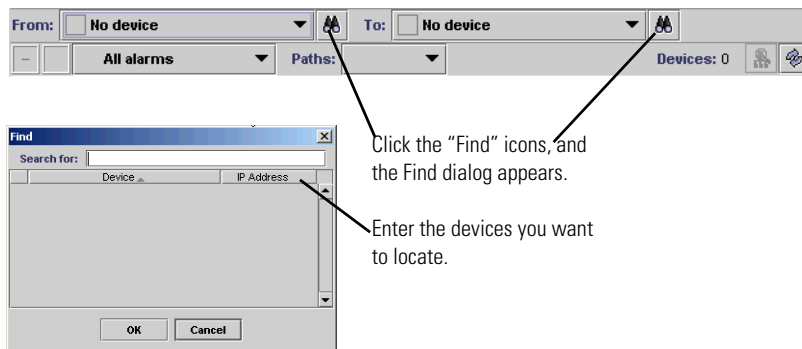
2 Click the first Find icon.

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.

The results

There are three panels of information available in the Service Analyzer:

- Path Alarms
- Path Graphs
- Summary Graphs

Path Alarms panel

The Path Alarms panel appears first, and shows the path between the two selected devices, and a table listing currently detected problems. In the "Paths" pull-down list, multiple views are available to display the data for different paths between the two devices.

Note: If there only a single path, as frequently occurs in many networks, it will be the only choice. The percentage indicates how frequently a path was taken. If there is a single alternative and yet the percentage is less than 100, it usually indicates a device in the path was off or broken for some time over the preceding 48 hours.

You will notice that the Service Analyzer 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.

Table 6-3: Service Analyzer Window (Path Alarms panel)

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

Path Diagram

Alarm List
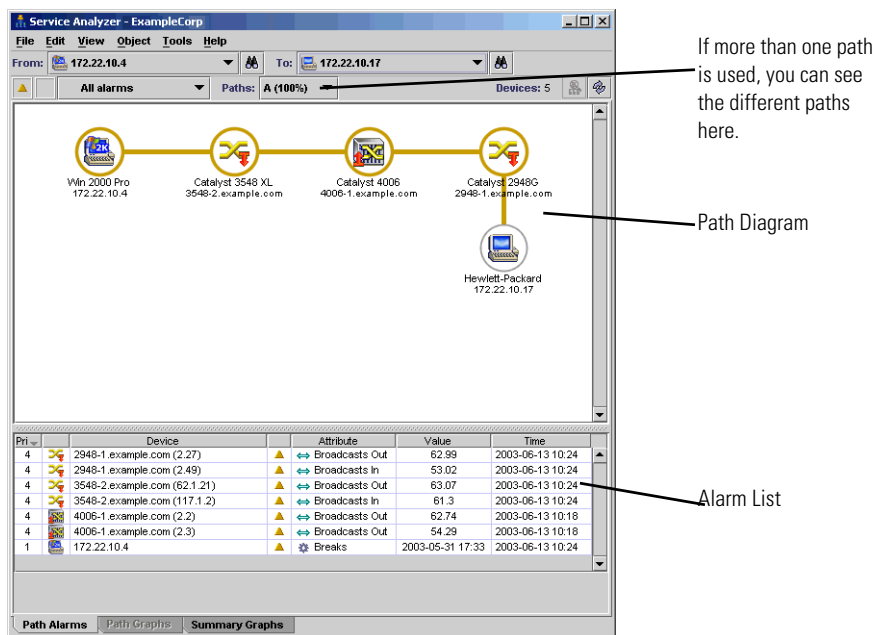
Double-clicking the lines opens Line Manager sessions. Double-clicking the devices opens Device Manager sessions.

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

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

Table 6-4: Problems detected on the path

Column	Notes	Example
Priority	—	—
Device Type	—	—

Table 6-4: Problems detected on the path (Continued)

Column	Notes	Example
Device (Port)	double-click to open the Device Manager	rbuffin.example.com (1)
State	—	—
Attribute	attribute name	Errors In
Value	For more information on the attributes, see the *Reference Manual*.	2.07 frames/sec.
Time	the time it was last polled	—

You can look at the Path Graphs and Summary Graphs to analyze the data from connection to connection.

Path Graphs panel

The Path Graphs panel shows the path diagram in a single vertical line along the left side of the window. On the right side, there are graphs representing each portion of the path. The graphs shown depend on which type of fault you have selected in the pull-down list in the Service Analyzer toolbar.

Note: For Collision and Errors, graphs are shown both for devices and the ports on those devices. The inbound port is shown, then the device, then the outbound port. (The device at the start of the path does not show an inbound port; the device at the end does not shown an outbound port.)

Note: For Delay and Jitter, graphs are shown for inbound and outbound ports.

Note: For Utilization and Broadcasts, there are a possible four graphs per device. Graphs for the inbound and outbound ports of a device are shown, and for each port, utilization to and back are shown.

Note: For Packet Loss, graphs are shown for all devices on the path.

Summary Graphs panel

The Summary Graphs panel shows a summaries of the entire path for the following alarm categories:

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

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

Find

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

Button		Function
	Find a Device on page 85	Allows you to search for a device by a basic attribute, such as Host Name, IP or MAC address, Net BIOS name, asset tag, or title.
	Find a Port on page 86	Allows you to search for a port by basic device attribute and port attribute (port index or description)
	Advanced Find on page 87	Allows you to use a wildcard to search on other attributes of a device. A description, contact, location, name (from SNMP), family, model, OS, application (from rule base) can all be used.
		Find devices with: allows you to identify the type of information on which you want to search. From the drop down list, you have the choice to search by model, operating system, application, and SNMP information.
		that: allows you to specify the type of query. The drop down list allows you to select: contain, begin with, end with, match exactly, match with wildcard, match using a regular expression.
		the text: allows you to enter a description of the device or devices you are trying to find.

If you have a map open, Network Discovery locates a found device in the map window.

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 Click the button for the Find panel you want to open **Device, Port** or **Advanced**.

3 Enter the search criteria.

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

Figure 6-5: The Find Window

Device Find with Basic attributes

Device Find for a port

Device Find for advanced search
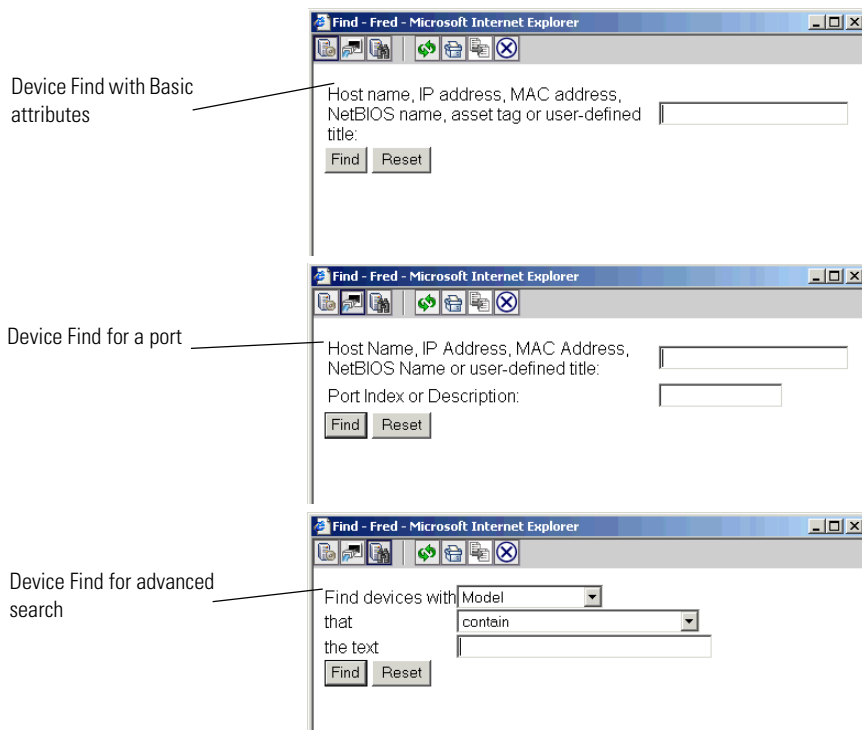
Find a Device

Searches for a device based on its name, title, address, NetBIOS name, or asset tag.

The search stops at the first successful category.

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

Table 6-5: Device search results

If the number of devices found is	Network Discovery does this:	You do this:
0	displays the message "not in database"	try entering the name differently
1	opens a Device Manager	—
2–35	displays a list of all results	click the linked title of one device in the list to go to the Device Manager
36 or more	displays a list of the first 35 results and a message that some results are not displayed	■ click the linked title of one device in the list to go to the Device Manager ■ narrow your search and try entering the device again

Limits
- *Input:* "localhost" | "nmc" | MAC address | IPv4 address | domain name | system-assigned title | user-assigned title | asset tag | NetBIOS name (network) | NetBIOS name (scan)
- *Output:* 0–35 results

Procedural alerts
- To find the Peregrine appliance, enter "nmc" or "localhost".
- To find multiple devices in the Network Discovery database, enter the first letter of a title or the first number of an address.

Important: Only the options that have been selected in **Administration** > **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.

Find a Port

Searches for a specific port of a device.

Table 6-6: Port search results

If the number of ports found is	Network Discovery does this:	You do this:
0	opens a Device Manager	—
1	opens a Port Manager	—
2–35	displays a list of all results (multiple devices, or multiple ports on a device)	■ click the linked title of one port in the list to be taken to the Port Manager ■ click the linked title of the device to be taken to the Device Manager
36 or more	displays a list of the first 35 devices and a message that some devices are not displayed	■ click the linked title of one port in the list to be taken to the Device Manager ■ narrow your search and try entering the port again

Limits   **Input**

- Port number
- Port description

Advanced Find

Searches for a device based on the contents of its SNMP MIB or Rulebase data.

Table 6-7: Advanced device search results

If the number of devices found is	Network Discovery does this:	You do this:
0	—	try entering the name again
1	opens a Device Manager	—
2–35	displays a list of all results	click the linked title of one device in the list to be taken to the Device Manager
36 or more	displays a list of the first 35 results and a message that some results are not displayed	click the linked title of one device in the list to be taken to the Device Manager~narrow your search and try entering the device again

Options
- Family | Model | Operating System | Application | SNMP Description | SNMP Contact | SNMP Name | SNMP Location
- Begins with | Ends with | Contains | Exact match | Match with wildcards | Match using a regular expression

Table 6-8: Wildcard characters

Option	Purpose	Example
?	Any single character	"gr?y" finds "gray" and "grey"
*	Multiple characters	"E*t" finds "Ethernet"

Note: Searches are not case-sensitive.

The "exact match" is inexact—case is not matched.

The "regular expression" is irregular—case is not matched.

Limits
- The device has to be active in the database.
- *Output:* 0–35 results

Administration

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

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

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

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

7 Customizing Your View of the Network Map

CHAPTER

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

Administrator or IT Manager have the option of changing System Properties. These System Properties will effect all accounts and all map configurations.

Topics in this chapter include:

- *Customizing for all accounts* on page 92
- *Customizing for IT Manager and Administrator accounts* on page 100

Customizing for all accounts

The following customization changes only affect map configurations of the person who makes them, unless the user has an IT Manager or Administrator account and makes system-level changes. For more information on map configuration files, see *Organizing Map Configuration Files* on page 117.

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

Renaming an object

You can give an object a descriptive title instead of the IP address, MAC address, or domain name. The new title will affect all of your map configuration files.

Note: If you have an IT Manager or Administrator account, you will see two tabs in the Properties dialog: My user properties and System properties. The user properties will affect only your account, but the system properties will affect all accounts.

To rename an object

1 With a device selected, **Object** > **Properties**.
2 In the Properties dialog, enter a custom title in the "Device title" field.
3 Click **Apply**.
4 Click **OK** to close the dialog.

To reset to the default title

1 Click the "Default" check box.
2 Click **Apply**.
3 Click **OK** to close the dialog.

Changing the priority of a device

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

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

Note: If you have an IT Manager or Administrator account, you will see two tabs in the Properties dialog: My user properties and System properties. The user properties will affect only your account, but the system properties will affect all accounts.

Warning: Warning for IT Manager and Administrator accounts. If you are changing the system-level priority of a device, you may affect your event filters. (For more information on event filters, see *Setting up Event Filters* on page 137.)

To change the device priority

1 With a device selected, **Object** > **Properties**.
2 In the Properties dialog, select a priority from the pull-down list in the "Device priority" field.
3 Click **Apply**.
4 Click **OK** to close the dialog.

To reset to the default priority

1 Click the "Default" check box.
2 Click **Apply**.
3 Click **OK** to close the dialog.

Customizing how you see the map

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

Changing the line style

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

To change the map line style

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

A dialog appears, from which you can change the line style.

2 Click one of the following:

- **Step**
- **Straight**
- **Zigzag**
- **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 scale

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

Change scale for all windows

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

To change the map scale preference (for all windows)

1   **Edit** > **User Preferences** > **Map**.

2   Enter a value between 1 and 300 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 two other options, described below.

To fit the map to your window

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

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

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   **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 **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 **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. This will affect all your map configuration files.

To truncate object titles

1 **Edit** > **User Preferences** > **Map**.

2 Click the box beside **Truncate object titles**.

Open Health Panel with Network Map

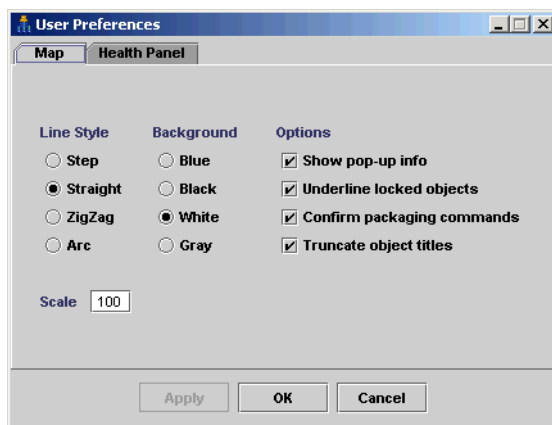**Note:** This setting does not affect the Aggregate Health Panel.

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 **Edit** > **User Preferences** > **Health Panel**.

2 Click the box beside **Open Health Panel with Network Map**.

Figure 7-1: User Preferences dialog

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 **View** > **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 **Object** > **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.

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, *Customizing for all accounts* on page 92.

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 a device icon and tag* on page 101	YES	■ 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 111	NO	NO
tag	*Changing a device icon and tag* on page 101	—	—
derived title (devices)	see **Administration** > **System preferences** > **Display preferences**	YES	—
title	see *Renaming an object* on page 92	system - YES user - NO	—
priority (devices)	see *Changing the priority of a device* on page 93	system - YES user - NO	whether event filters are applied (all accounts)
to top object	see *Placing an object at the top of the map window* on page 98	NO	—

Changing a device icon and tag

If you have an Administrator or IT Manager account, you will see two panels in the Device Properties dialog:

- My User Properties
- System Properties

My User Properties effect only your account. System Properties effect all accounts.

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

Warning: If you change a system-level device icon and priority, it will affects your event filters. See *Setting up Event Filters* on page 137.

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

Note: Changing a device icon can change how it is packaged. Certain icons are 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**.

To change a device icon and/or priority

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

The Device Properties dialog appears.

2 Click the System Properties tab.
3 From the pull-down list, select a new icon for the device.
4 If you want to change the device tag, enter your custom text.
5 Click **Apply**.
6 Click **OK**.

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

Figure 7-2: Device Properties window
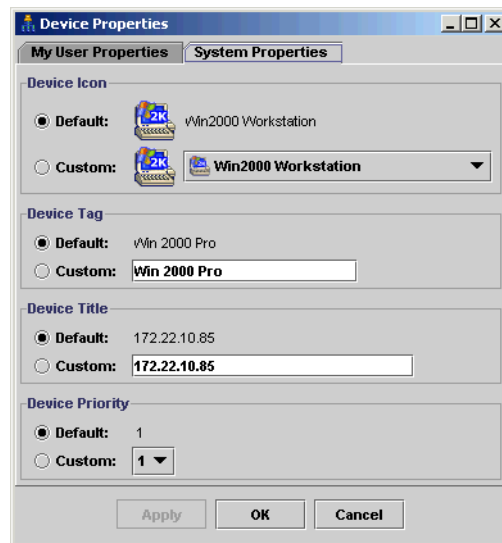
To reset the device icon and/or device tag to the default

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

The Device Properties dialog appears.

2 Click the System Properties tab.

3 Select "default" in the Device Icon section of the screen.

4 Select "default" in the Device Tag section of the screen.

5 Click **Apply**.

6 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 applies across all map configurations for all accounts. These are universal changes.

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

There are two tabs available, one for device types, and one for line types.

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.

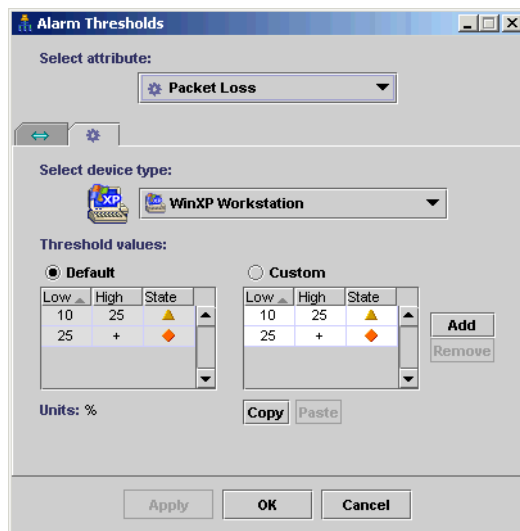4 Select a line or device type from the pull-down list.

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

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

Figure 7-3: Alarm Thresholds (Device Types)

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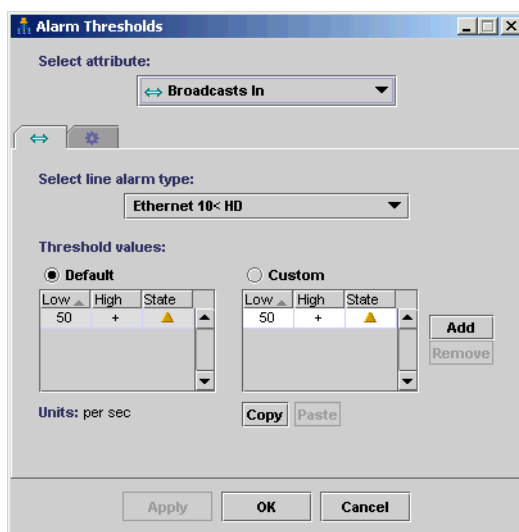
To change the Device Alarm Thresholds

1 Select an attribute from the pull-down list.

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

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

Figure 7-4: Alarm Thresholds (Line Types)

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

To change the Line Alarm Thresholds

1 Select an attribute from the pull-down list.
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.

8 Packaging Your Network

CHAPTER

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

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

Topics in this chapter include:

- *How packaging works* on page 108
- *Changing the automatic packaging preferences* on page 114
- *You can request the creation of packages* on page 110
- *You can create your own multi-object packages* on page 111

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
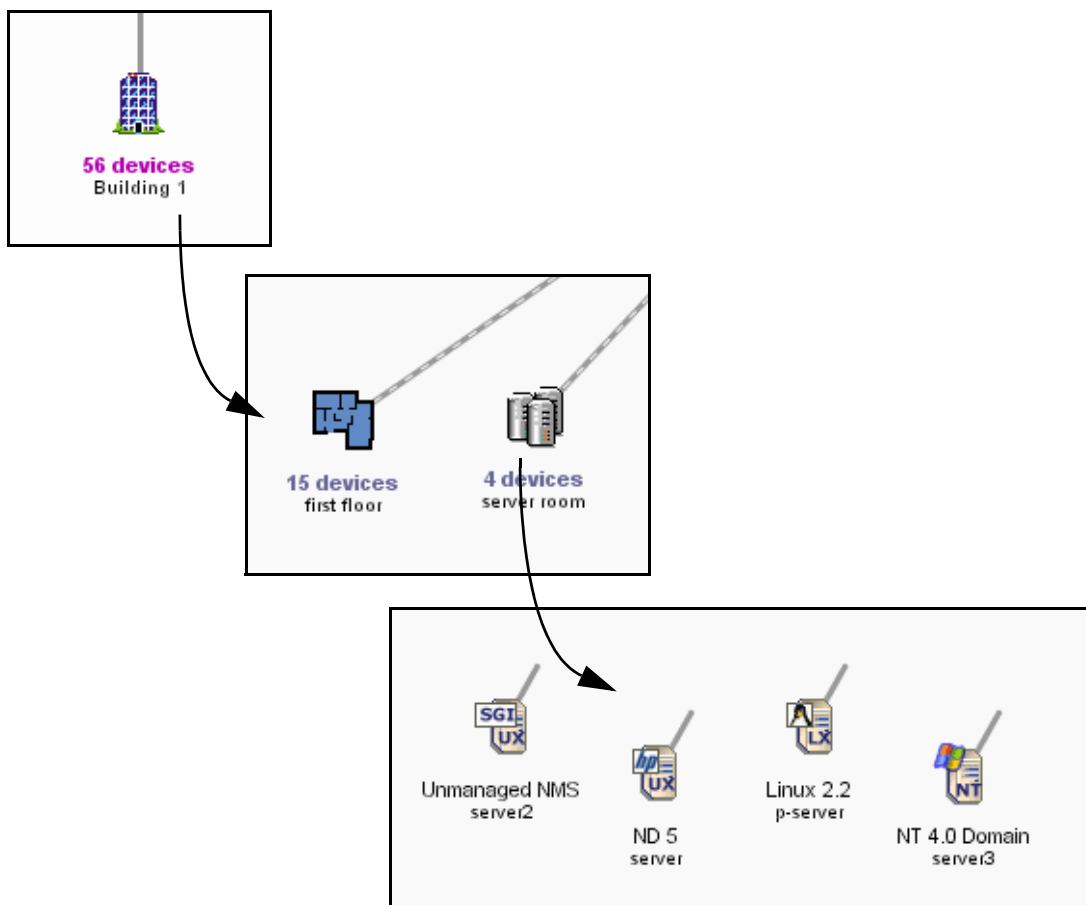
You can request the creation of packages

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 **View** > **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 **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** > **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**.

To create a new package without any objects in it

1 From the **View** menu, click **Create Package**.

2 Add objects by dragging icons into the new package.

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

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

You can also unpack your packages

To move the contents of the active package up one level

▶ From the package window, click **View** > **Unpack**.

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 **View** > **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 **Unpack**.

To empty one package

▶ From any map window, with a package selected, click **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 Network 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 (Up a Level, **Promote**), or has had its package removed (**Unpackage**).

Figure 8-2: Example of a Locked Device

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

Network Discovery creates some automatic packages. Whenever you use the Pack or the Unpack All commands, Network Discovery will recreate 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

▶ **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.

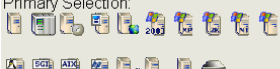### To create automatic packages of a particular type

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

9 Organizing Map Configuration Files

CHAPTER

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

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

Topics in this chapter include:

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 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 characters long. 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**.

Note: **Save As Prime** is not available when using the **Forecast** command to view the Network Map.

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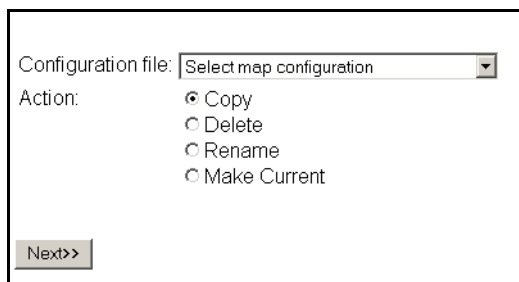
Note: Close your map before performing any of these procedures.

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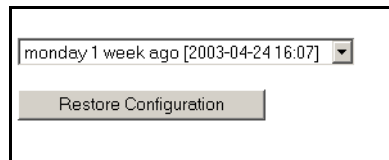
1 Click **Administration** > **Data management** > **Restore prime map configuration**.

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

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.

Entering the e-mail address

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

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

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

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

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

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

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

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.
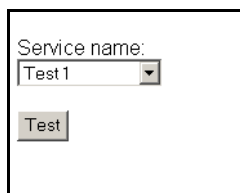
3 Click **Test**.

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

Test

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.
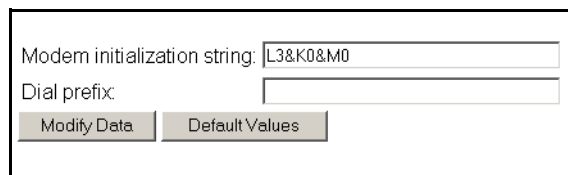
To modify modem properties

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

Modifying account profiles

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

To modify an account profile

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

To enable paging through an e-mail gateway

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

To enable direct alphanumeric paging

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

Figure 10-5: Modify contact data

E-mail address:	admin@example.com
Pager e-mail address:	admin_pager@example.com
Pager number:	5551212
Pager Service Provider:	Test 2

Modify Contact Data

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 137.

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?

Confirm

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.

OK
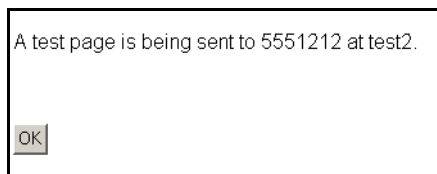
Modifying information for a service provider

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 Setting up Event Filters

CHAPTER

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 Service Center. 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 71 and the *Reference Manual*.
Understand how to configure Network Discovery to send tickets to ServiceCenter	See *Opening Tickets in ServiceCenter* on page 157.
Hardware Issues	
Set up and test your pager equipment (hardware and software)	See *Setting up Paging* on page 127.
Account Issues	
Set up account contact information	**Administration** > **Account administration** > **Account properties.** See *Modifying account contact information* on page 29.
Set up your Network Discovery Administrator e-mail address	**Administration** > **Appliance Management** > **Administrator e-mail address.** See the *Setup Guide*.
Network Map Issues	

Concept	Commands and where to get more information
Change device priorities	*Changing the priority of a device* on page 93
Changing alarm thresholds	*Changing Alarm Thresholds* on page 102

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:
  - Network Discovery Administrator e-mail address
  - SMTP server
  - SNMP traps setup (only if you plan to use SNMP traps)
  - Pager setup (hardware installation and pager service provider information)
  - 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.

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** > **Properties**.

4 In the System Properties tab, 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
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

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** > **Properties**.
4 In the System Properties tab, 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

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** > **Properties**.

4 In the System Properties tab, 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

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 *Opening Tickets in ServiceCenter* on page 157).

To set the device priority

1 Open a Network Map session.

2 Find an important device and select it.

3 Click **Object** > **Properties**.

4 In the System Properties tab, 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

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 Event Type list box.

4 Select one or more options from the Priority list box.

5 Select one or more options from the Device Type list box.

6 Select one or more options from the Line Alarm list box.

7 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 Opening Tickets in ServiceCenter

CHAPTER

> **Important:** This feature will only work with Network Discovery version 5.1, and ServiceCenter version 5.1.

Network Discovery can be configured to automatically open tickets in ServiceCenter using event filters. You must have your event filters set up properly in order for this feature to work (see *Setting up Event Filters* on page 137).

Network Discovery uses the following events to open tickets in ServiceCenter:

- NDpmo
- NDpmc
- NDicma

When the problem occurs, a ticket is opened. When the problem is returned to an OK state, the ticket is automatically closed.

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: The ticket number will only appear in the pop-up if you have a ticket open for the attribute selected in the map pull-down list. (Report options such as "Exceptions" and "Open Tickets" cannot have tickets opened in ServiceCenter).

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 65).

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** > **ServiceCenter configuration** > **ServiceCenter settings**.
2 Enter the settings for your ServiceCenter configuration.

Setting	Explanation
Host name of IPv4 address	The address of your ServiceCenter product.
Port	The port for accessing ServiceCenter.
Username	Your ServiceCenter account name.

Setting	Explanation
Password	Your ServiceCenter account password.
Request Timeout	Optional.
Category, Subcategory, Site Category	These are required fields in ServiceCenter tickets.
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.

3 Click **Change**.

Figure 12-1: ServiceCenter configuration

To test your connection to ServiceCenter

1 Click **Administration** > **ServiceCenter configuration** > **Test ServiceCenter**.

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.
- moving 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 12-2: Deleting Tickets

There are 65 tickets open.

Delete Tickets
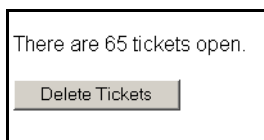
13 Adding and Replacing Devices

CHAPTER

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* on page 162
- *Adding a device* on page 162
- *Replacing a device* on page 164
- *Changing the IP address of a device* on page 165
- *Changing the cards or ports in a device* on page 165
- *Activating devices* on page 166

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 **Network**.

6 Click **Update**.

Network Discovery begins network discovery on the device immediately.

With the same IP Address as a deactivated device

If a device has been deactivated, and you are using that IP address for a new device, it is best to purge the old device. To purge the device, see *Deleting Data, Connections, and Devices* on page 169.

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

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

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.

Replacing a device

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

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

With an identical device

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

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

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, it always best to purge the old device before adding the new device.

Changing the IP address of a device

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

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

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

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

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

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

Changing the cards or ports in a device

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

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

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

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

1 Physically remove the device from your network following your company's standard procedures.

2 Locate the device on the Network Map using the **Find** tool.

3 With the device icon selected, **Object** > **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 173.

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 Deleting Data, Connections, and Devices

CHAPTER

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

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

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	YES	YES	YES
Events	YES	YES	YES
Forecast databases	YES	YES	YES
Accounts	—	YES	YES

Table 14-1: Options for deleting data (Continued)

What gets deleted	Network data	Network data plus accounts	Network data, accounts, config, backups
Map configurations	—	YES	YES
Devices for any remote appliances[a]	—	—	YES
Administration configuration	—	—	YES
Internal backups	—	—	YES

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

Delete Data

Deleting connections

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

You can choose to delete:

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

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

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
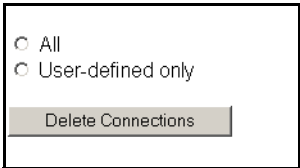
Removing devices

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	2 stages ■ deactivate ■ purge
manual	an IT Manager or Administrator user	3 methods ■ hide ■ deactivate ■ purge

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

Action	Hide	Deactivate	Purge
device removed from Network Map	YES	YES	YES
device can be recovered if seen	—	YES	__a
"delete" event generated	YES	YES	YES
device statistics deleted	YES	—	YES
device events deleted	YES	—	YES

a Once purged, 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. The length of this interval is specified in **Administration** > **System Preferences** > **Expiry**. When the deactivation interval ends, the device is made inactive.

Once the device is inactive, the purge interval begins. The length of this interval depends is specified in **Administration** > **System Preferences** > **Expiry**. When the purge interval ends, the device and all its associated data are removed from the database.

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.

Figure 14-3: Default values for automatic removal

managed   12 weeks total

        8 weeks   4 weeks

unmanaged   5 weeks total

    1 week   4 weeks

☐ time to be deactivated   ◼ time to be purged
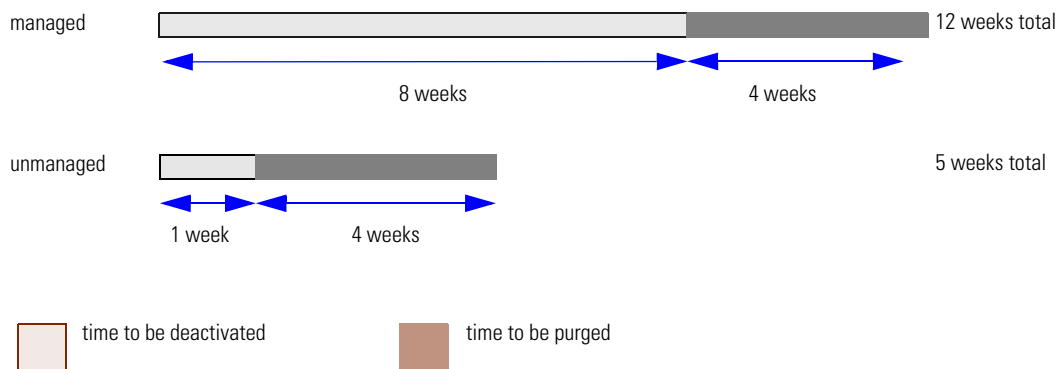
Changing the device expiry intervals

Device expiry has two steps: deactivation and purge.

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.

Inactive devices disappear from the Network Map and reports, but their statistical information is preserved in the event that the devices are returned to an active state before they are permanently purged. When the device is inactive, it is considered "deactivated" and appears in the list of devices at **Status** > **Deactivated Devices**.

Changing the device deactivation and purge intervals

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.

Figure 14-4: Device Deactivation Intervals and Purge Intervals

To change the device deactivation and purge intervals

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

2 Enter the values for the time for managed, unmanaged and scanner-only devices.

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 174), 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 166.

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 Vacations and Weekends

CHAPTER

This section is for the Network Discovery Administrator only.

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

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

Topics in this chapter include:

- *Before you go away* on page 180
- *When you come back* on page 181

Before you go away

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

Set the Deactivation and Purge intervals

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

To change Deactivation and Purge Intervals

Administration > **System preferences** > **Expiry.**

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

For more information, see *Changing the device expiry intervals* on page 174

Change who will be notified when events occur

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

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

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

Note: You must already have set up your substitute's account. You may have to give your substitute Administrator account privileges. For instructions on setting up accounts, see *Setting up Accounts* on page 23

When you come back

You can monitor events in a few different ways, depending on what you want to see:

- Check the Network Map, Health Panel, and Alarms Viewer to see current network faults.
- Use the Events Browser to view alarms specific to particular times.
- View Fault Summary reports to view alarms over longer periods of time.

When you come back after a weekend, check to see if anybody added, removed, or modified any devices in your network.

Top priority

Check for any current emergencies that need your attention right now.

- Check the Network Map, Health Panel, and Alarms Viewer for serious alarms to major devices.
- For any problematic device, check the Device Manager and Statistics for that device.
- Use the Service Analyzer tool to check paths for devices about which the users are concerned.
- Check Reports for major issues from the last few days.

Second priority

Once you have dealt with the emergencies, you will want to check on the other problems that happened while you were away, specifically on priority 3, 4, 5, and 6 devices. These may be intermittent problems that can cause network delays or outages in the future.

Some good questions for your substitute administrator would be:

- How long did it take to fix them?
- What was the cause of the problem?
- Who fixed them and how?

Other ways to check for the problems would be to check:

- the Events Browser for alarms before a certain date

- Performance Summary and Fault Summary reports for all types of alarms

- other reports depending on the contents of your network

Third priority

You will likely want to check what devices have been added, deleted, or moved in your network while you were gone. This will allow you to see how the contents of your network have changed (if anyone has added or removed network equipment without informing you).

Check the Health Panel to see:

- what devices have been added recently (Device Adds/Deletes)

- what devices have been moved recently (Device Moves)

- what devices have not been seen recently (Not Recently Seen)

Checking individual devices

If you are concerned about any devices in particular, you should check the Device Manager and Port Manager windows for those devices. Concentrate on the Statistics panel, but you would also want to check the information on the State and Events panels.

16 Using an Aggregator

CHAPTER

If you have received an Aggregator license, this chapter will show you how to set up and use the Network Discovery Aggregator. To use the Aggregator, all of your Peregrine appliances must be at least 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 16-1: Simple conceptual network map
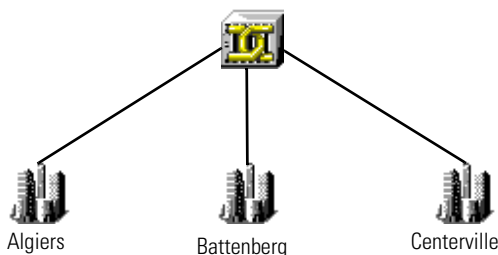
Ideally, you would have purchased 4 Peregrine appliances: one for each office, and one to act as an Aggregator for the central office (in Centerville).

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

Figure 16-2: Network map with Peregrine appliances and routers

Algiers

Battenberg

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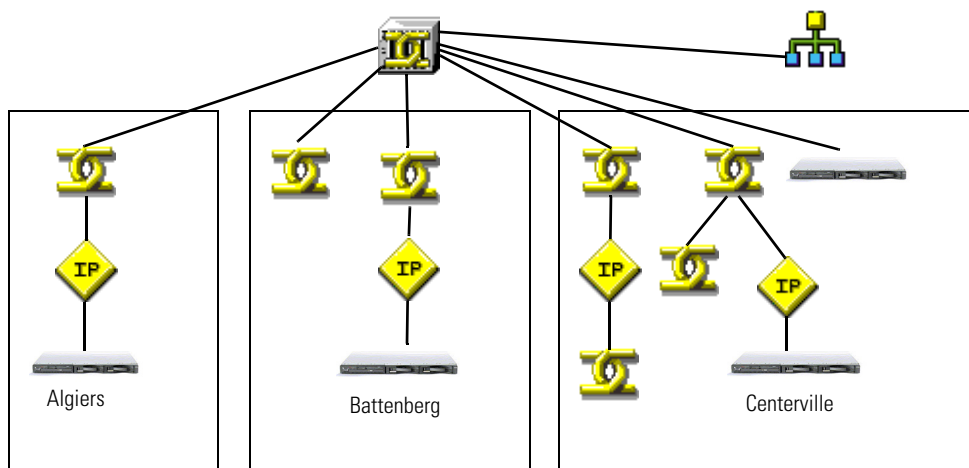
Tip: If the Network Map for your Aggregator does look like this, you can right-click on each Peregrine appliance to open map windows for each appliance.

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 16-3: Aggregate Toolbar

Extra row of buttons shows that this Toolbar belongs to an Aggregator

The extra Aggregate-specific buttons are listed in the following table. Note the "globe" symbol in each icon.

Table 16-1: 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.
	Remote Appliances	Opens a page showing all the remote appliances that are configured to work with the Aggregator.
Appliance: Marbles	Appliance pull-down list	Changes the context of the Toolbar buttons.

The buttons in the bottom row are the same as the buttons on a single appliance Toolbar. They affect only the Peregrine appliance you have selected from the Appliance pull-down list.

Setting up the Aggregator and remote appliances to work together

For the Aggregator to work, you must prepare the Aggregator and you must prepare each individual appliance. You give the Aggregator:

- the IP address of the remote appliance
- the remote account
- the Aggregate health update interval
- the Aggregate events update interval
- proxy use

On each individual Peregrine appliance you set up an account that allows access to the Aggregator.

To set up the Aggregator to access a remote appliance

1 On the Aggregator, click **Administration** > **Remote appliance administration** > **Add a remote appliance**.

2 Enter the IP address and the name of the remote appliance.

3 Click **Add**.

4 Click **Modify Properties**.

5 Enter a remote account (example, "admin") to collect data for the Aggregate Health Panel.

6 Select an Aggregate health update interval.

   Note: Here are some things to consider. More frequent updates use more more bandwidth.

7 Select an Aggregate events update interval.

   Note: If you are using proxy services, be sure to read *Using Proxy Services* on page 197. If you are not using proxy services, skip step 8 and go to step 9.

8 If you are using proxy services, select one of the proxy options.

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

9   Click **Change**.

Setting up the remote appliances for access

In order for the Aggregator to access Peregrine appliances in your network, you must have identical accounts on each Peregrine appliance that you want to aggregate.

Important: Repeat this procedure on each Peregrine appliance.

For example, if you have an Administrator account "kevin" on the Aggregator, you must have an Administrator account "kevin" on each remote appliance. The two accounts must have the same password. If the Aggregator and the remote appliances do not have identical accounts:

- the Aggregator and the remote appliances will not be able to communicate with each other
- you will not be able to access the remote appliances through the Aggregator

This procedure explains the minimum setup required to access the remote appliances. For more information on account setup, see *Setting up Accounts* on page 23.

Important: The account used to see Aggregator data must be exactly the same on each Peregrine appliance. The accounts must have the same name (for example, admin), password, and account type (for example, Administrator).

To add an account

1   On the remote appliance click **Administration** > **Account administration** > **Add an account**.

2   Enter a login name.

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

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

Note: Uppercase letters are not acceptable.

3 Click **Add Account**.

A new screen appears, where you can modify account properties, contact data, and the password.

4 Click **Modify account properties**.

5 Select an account type from the list box.

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

6 Enable the account for Web Access by selecting "Yes".

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

Note: If no password is given, the account cannot be used to log in, even when login status is set to "yes".

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

8 Click **Modify Properties**.

A new screen appears, where you can modify account contact and the password.

9 Click **Modify account password**.

10 Enter the new password in the first field.

Do not enter the current password (if any).

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

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

11 Enter the same new password in the second field.

Entering the same password twice helps guard against typing errors.

12 Click **Modify Password**.

You have finished setting up the account on one remote appliance. Now, you must repeat this procedure for each remote appliance the Aggregator needs to access.

Note: When you access a remote appliance by means of the Aggregator, the user preferences set on the Aggregator override those on the remote appliance.

Navigating through multiple appliances

There are two ways to switch appliance views:

- using the appliance pull-down list on the main Toolbar
- using the Remote Appliances list from the 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 16-4: Remote appliance pull-down list

Appliance: Marbles ──────── Remote appliance in the pull-down list (there is no asterisk (*)
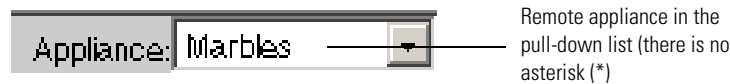
Using the Remote Appliances list

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 16-5: Home and Home Base
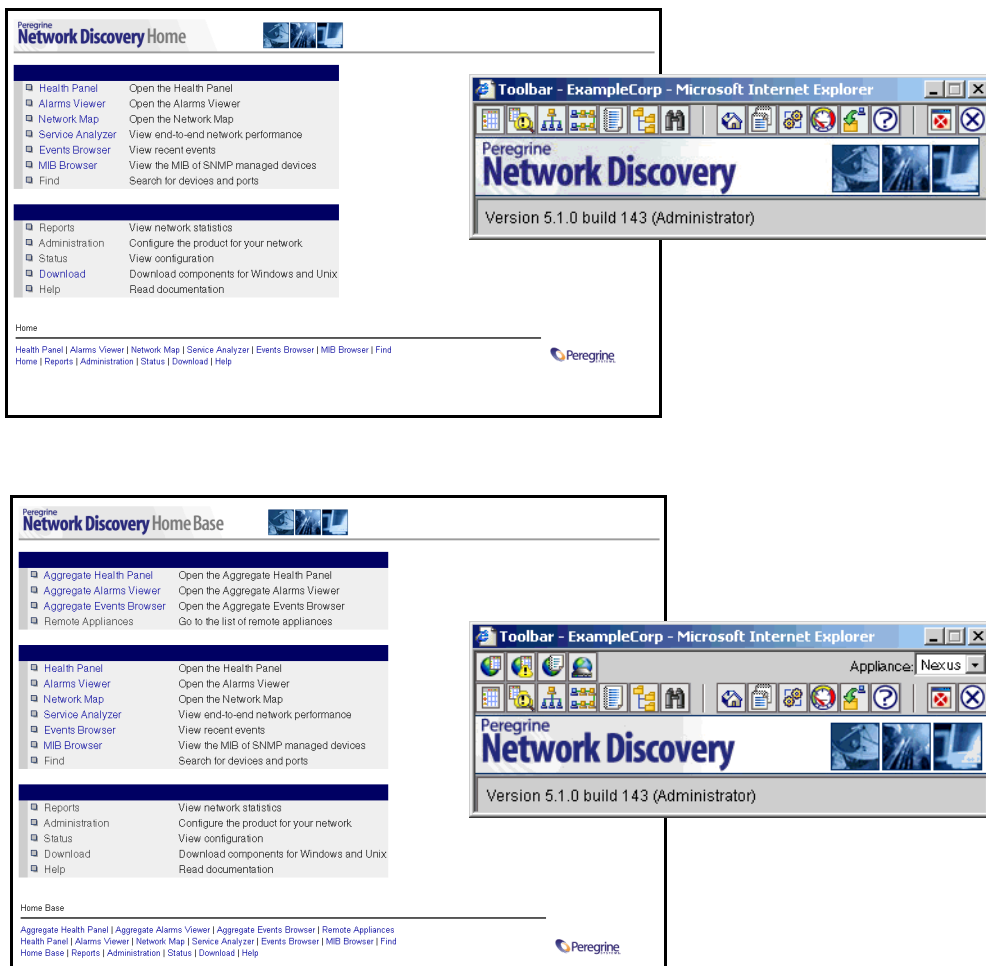
Using the Aggregate Health Panel

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

You can click on the report buttons to see complete lists of all events in the entire network. If you were looking at a regular Health Panel for one appliance, you would only see faults for a portion of your network.

Note: You can tell what Health Panel you're looking at by the report banner. If it is the 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 49.

Figure 16-6: The Aggregate Health Panel

Banner says "Aggregate Health"

Globe symbol also indicates Aggregate Health Panel

Alarm		■	◆	▲	✳
◆	⇔ Line Breaks		27		
◆	⇔ Utilization		5		
◆	⇔ Delay		4		
▲	⇔ Broadcasts			290	
◆	⇔ Errors		1		
◆	✿ Device Breaks		52	23	
■	✿ Disk Utilization	2	11	111	28
■	✿ CPU Utilization	1		2	3
▲	✿ Load Average			7	
■	⇔ Port MTTR	86	27	15	28
■	⇔ Port MTBF	7			
✳	⇔ Port Adds/Deletes				11
✳	⇔ Port Moves				1
✳	⇔ PortChanges				42
■	✿ Device MTTR	270	80	72	57
■	✿ Device MTBF	42			
✳	✿ Device Adds/Deletes				538
✳	✿ Device Changes				43
◆	✿ Exceptions		35	26	182
✳	✿ Not Recently Seen				39
■	✿ Open Tickets	2	38	20	

Devices	Ports	Availability	Frames/s	Errors/s
5,042	2,824	93.84%	23,277	7.15

Aggregate Health - ExampleCorp

File   Edit   View   Tools   Help

CPU Utilization   1-6

◆   2   3:45 PM   ⇔

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. However, events from an aggregated remote appliance have "[via Appliance name]" in the device/port column; events reported by the local appliance do not.

The Aggregator updates events hourly (by default). Due to the time lag, events may not be completely up to date.

If aggregation is turned on, but no Aggregators have been set up, the aggregate Events Browser will look very much like the regular Events Browser except for the time delay.

The Aggregate Alarms Viewer

The aggregate Alarms Viewer is almost identical to the regular Alarms Viewer. However, alarms from an aggregated remote appliance have "[via Appliance name]" in the device/port column; events reported by the local appliance do not.

17 Using Proxy Services

CHAPTER

This chapter provides a cursory overview of the proxy services available with Network Discovery. You should have a high level of networking expertise to use this feature. If you are uncertain about how to set up this feature, you may want to contact Peregrine Systems Customer Support for help.

Warning: If you are unsure about how to use Proxy services, do not attempt to use this feature.

Topics in this chapter include:

- *Four examples* on page 198
- *Using the default—no proxy* on page 198
- *Proxy access through a remote appliance* on page 200
- *Proxy access through the Aggregator* on page 201
- *Proxy access through the Aggregator and remote appliances* on page 203

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 17-1: Possibility one—direct HTTP/Telnet access

Network Discovery Aggregator   Remote Peregrine appliance

Management
workstation   Printer
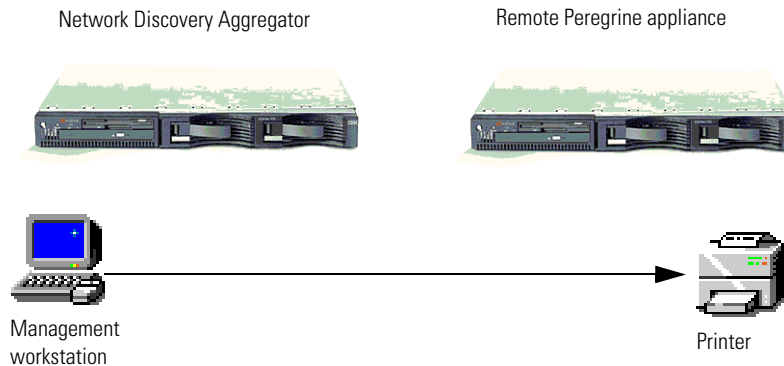
Description

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 17-2: Possibility two—through a remote Peregrine appliance

Network Discovery Aggregator   Remote Peregrine appliance

Management workstation   Printer
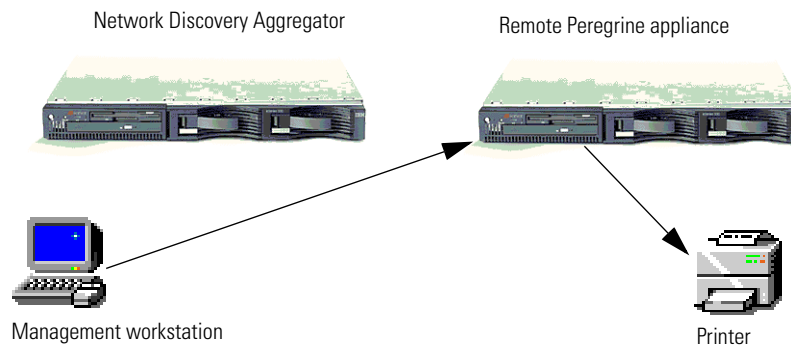
Description

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 17-3: Possibility three—through the Aggregator

Network Discovery Aggregator

Remote Peregrine appliance

Firewall

Management workstation

Printer
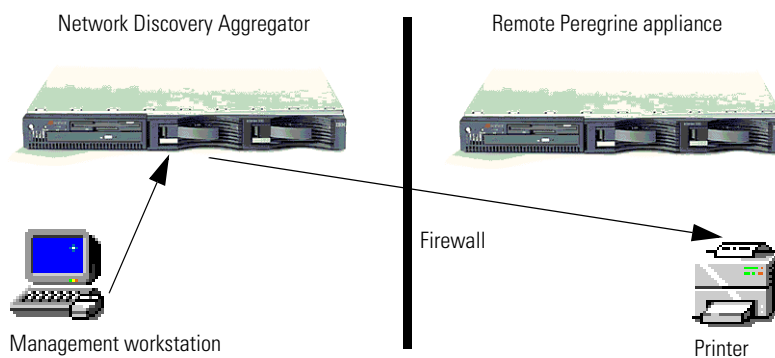
Description

Proxy through the Aggregator actually allows you to access the remote Peregrine appliance, which will access the device you want to see. In this case, a firewall is blocking your workstation's view of the remote Peregrine appliance, so you access the Aggregator first, and connect to the end device through the remote Peregrine appliances.

How to set it up

To set up on the remote appliance

Important: You must repeat this procedure on each remote Peregrine appliance in your network. If you do not set up all the remote Peregrine appliances, your proxy services will not work properly.

1 Log into the remote Peregrine appliance.

2 Click **Administration** > **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.**

9 Click **Change**.

Proxy access through the Aggregator and remote appliances

Figure 17-4: Possibility four—through the Aggregator and remote Peregrine appliances

Network Discovery Aggregator   Remote Peregrine appliance

Workstation   Printer
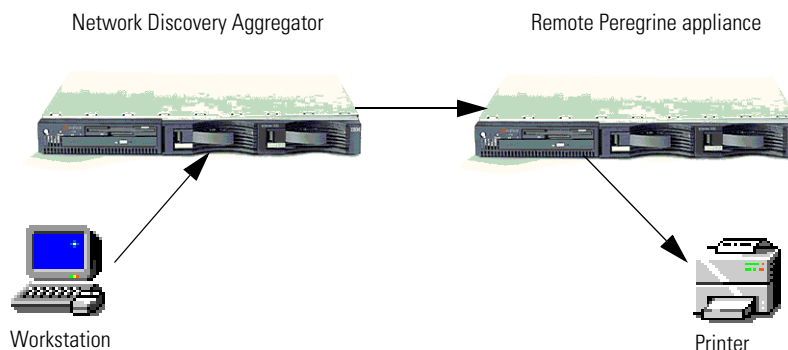
Description

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**.

18 Connecting with Another Management System

CHAPTER

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

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

Topics in this chapter include:

- *Connecting from Network Discovery to another system* on page 206
- *Connecting to Network Discovery from another system* on page 208

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 18-1: Setting up the Default URL

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

Change

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 206.

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**.

19 Viewer

CHAPTER

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 (.xml.gz 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.

Launching Viewer

The Viewer is accessible through the Device Manager.

Exiting Viewer

To exit Viewer on use one of the following methods:

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

Viewer user interface

In this section...

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 xml.gz-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.

```
File  Edit  View  Help
```
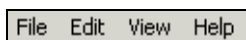
To open a menu:

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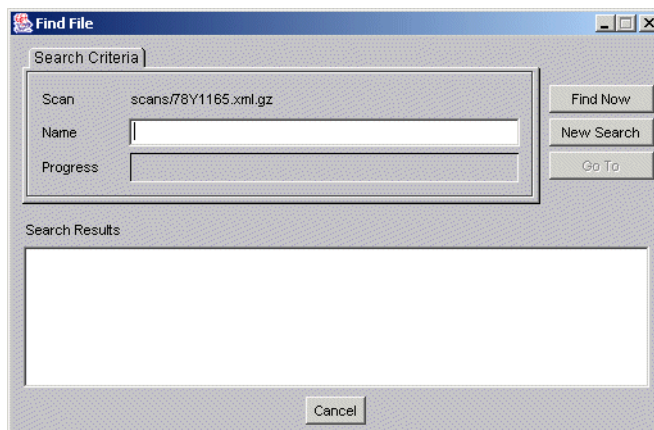
2 In the **Name** box type the name of the file you want to find. You can use DOS wildcard characters, (using * and ?) as well as normal alphanumeric characters.

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

Item	Description	Page Displayed
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.
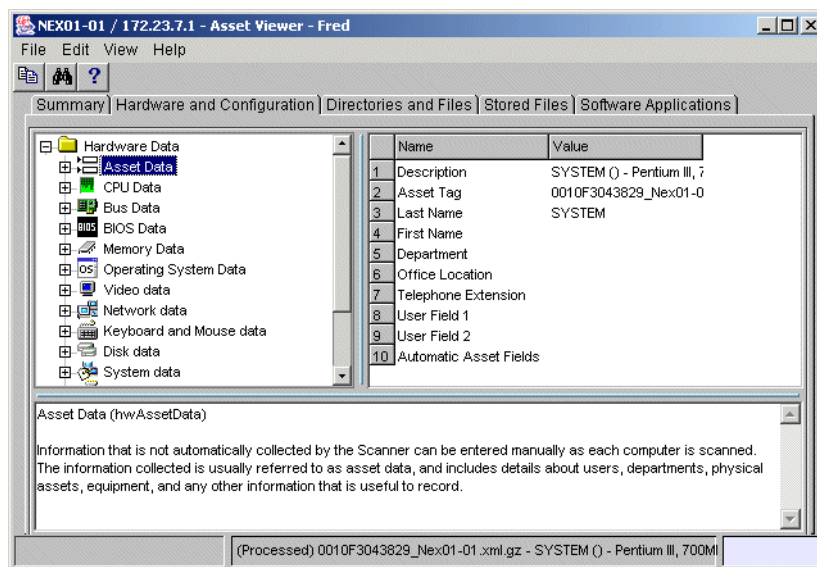
The Hardware and Configuration tab page layout

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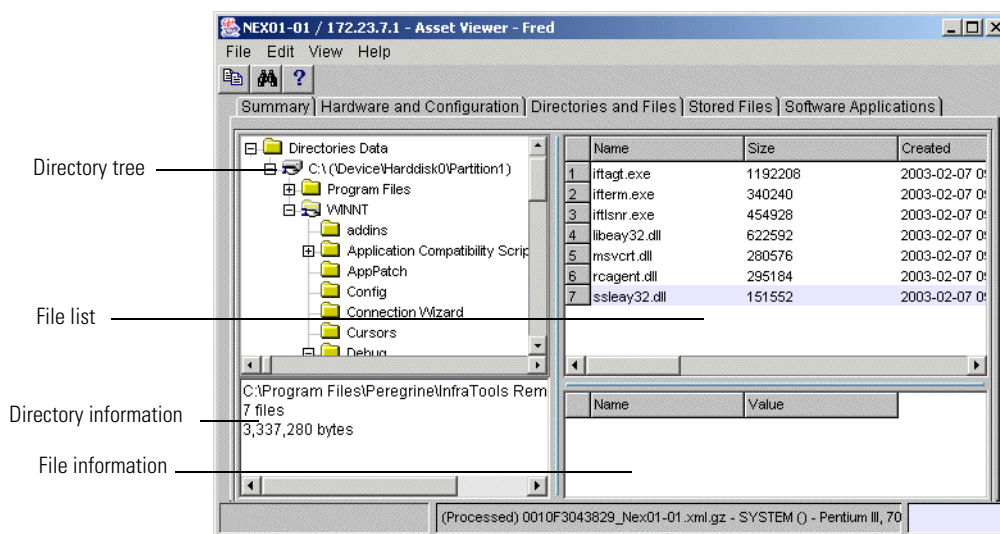
The **Directories and Files** tab page is split into four viewing areas (panes):

- 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.
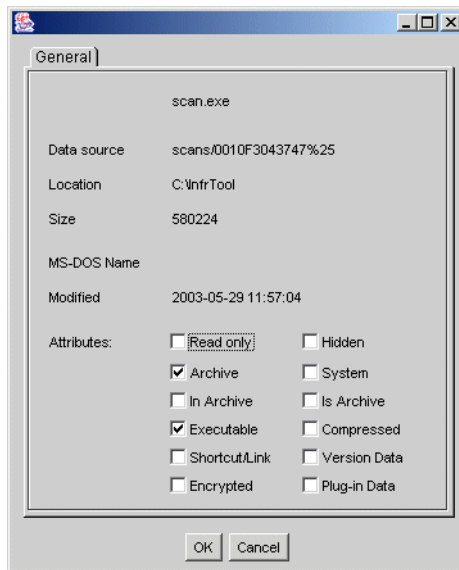
Icons used in the Viewer to denote directory status

Different icons are used to denote directory status as follows:

Icon	Directory status
	Indicates a shared directory.

Icon	Directory status
🚫	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 or Unix scans. Mount points are automatically filtered.
📁	In Unix scans, files (and directories) may be located on several different file systems. To link files that are in different file systems a symbolic link is made.
	This icon is displayed for directories that are symbolic links. You can follow the link by right-clicking on the directory and selecting the **Follow Link to** <**link**> option.

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.

Unix scans

For files in Unix scans, you can obtain link information about the file by right-clicking on the file and selecting the **Follow link** option.

This option is only available for files with the **L** attribute (indicates a symbolic link file). You can also do this by double-clicking on the file. The link information is displayed in the file information pane.

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.
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.
L	Symbolic link in Unix
	Files (and directories) may be located on several different file systems. To link files that are in different file systems a symbolic link is made.
	Symbolic links to files are not scanned but are stored with this attribute and are displayed in the directory tree of the **Directories and Files** page with a shortcut icon.
s	This is special case for Unix for SetUid files.
	In Unix scans, certain files have special attributes that mean that they run with root privilege. Such files are potentially a security risk and the Scanner assigns them the system attribute - **s**

Attribute	Meaning
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**.
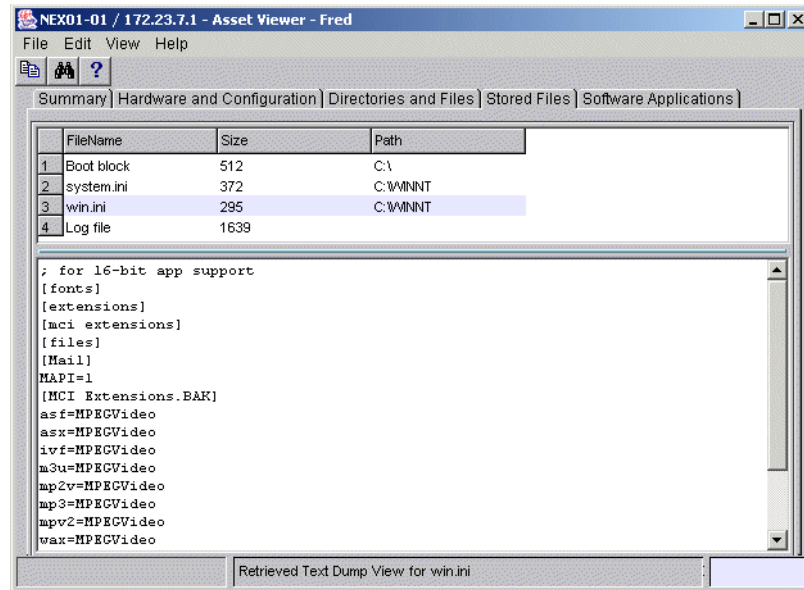
The Stored File tab page is split into two viewing areas:

- **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 the **Toggle Display Mode** command from the 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*.

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.

Index

device
    activating 166
    adding 162
    changing IP address 165
    changing ports 165
    changing priority 93
    deactivate 177
    deactivating 176
    hide 176
    not seen 60
    purge 177
    purging 176
    remove automatically 174
    removing 169, 176
    replacing 164
    title 57, 78, 86
Device (Find) 85
Device Manager 68
    changing default panel 26, 27, 37
device types 103
device, disconnecting 21
Directory 223
Disconnect command 62
disconnecting
    map session 21, 62, 63

E
Editing asset information 215
Element management 206
e-mail
    change account e-mail address 29
    change your own e-mail address 38
    test your e-mail address 40
evaluation periods 13
event entry 73
event filters 137
    definition 139
    delete 154
    examples 141
    list 154
    modify 153
    preparation 140
    reset to defaults 155
Events Browser 71–75
    Category 74

    event entry 73
    Limit 75
    Newer 75
    Older 75
Exiting viewer 210
expiry 174

F
faded icon 60
File attributes 217
File information 219, 221
File list 219, 221
File parameters 217
Find 83
    Advanced 87
    Device 85
    Port 86
Fit Map to Window 95
Fit Window to Map 95
Forecast 65
found objects 61
FSF 214

H
Hardware 210, 214, 215
Hardware information 215
HD Capacity 214
Health Panel 49, 54
    aggregator 194
    alarm list 50
    opening with Main Map 97
help format 27, 37
    change 26
help, Assistant window 27, 37
hiding devices 176
Home Base (Aggregator) 192

I
icons 55
    appearance 60
    blue line under icons 61
    changing 101
    changing size 94
    faded 60
    found 61