

Peregrine

Network Discovery Setup Guide

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

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

Peregrine Systems® is a registered trademark of Peregrine Systems, Inc. or its subsidiaries.

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

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

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

This edition applies to version 5.0 of the program, Peregrine's Network Discovery.

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



Table of Contents

Chapter 1	Welcome to Network Discovery	5
	Overview	6
	Setup overview	6
	Why it's important to do the preliminary work	6
	Collect information	7
	Prepare the network	9
	Check the management workstation	12
Chapter 2	Install and Start Network Discovery	15
	Install the hardware	16
	Connect the Peregrine appliance to the network.	16
	Connect a keyboard and monitor or a terminal directly to the Peregrine appliance 17	
	Connect a management workstation to the network	18
	Connect an Uninterruptible Power Supply (UPS)	18
	Connect data backup equipment and pager hardware	19
	Connect the Peregrine appliance to a telephone line	19
	Connect the Peregrine appliance to AC power.	20
	Start Network Discovery the first time	20
Chapter 3	Appliance Management	23
	Log in to Network Discovery	24
	How to shut down the Peregrine appliance	27
	The Home page	28
	The Toolbar	29

	Assign a system name, contact, and location	31
	Change the Peregrine appliance community strings	32
	Set the time zone	33
	Enter the domain name server	34
	Enter the host name	35
	Enter the Workgroup name.	36
	Enter the Administrator e-mail address	37
	Enter the SMTP server	38
	Set the system time	39
	Change the default Admin password	41
	About disabling UPS and backup warnings	43
Chapter 4	Licenses	45
	How it works	46
	Request a new license	46
	Install the new license	47
Chapter 5	Set up Network Discovery	49
	How it works	50
	Set up the IPv4 range(s) to discover	50
	Set up the IPv4 range(s) to avoid	52
	About community strings	52
	Activate your proposed changes	53
Chapter 6	Refining Network Discovery	55
	A precise matrix of network discovery	56
	A tree of IPv4 ranges.	56
	Property Groups	59
	Network Property Groups	60
	How to use Network Property Groups	62
	Create or modify a Network Property Group	63
	Apply a Network Property Group to a range	65
	Community Property Groups.	65
	More on community strings	66
	Property sets are a shortcut	69
	Reviewing and activating your configuration changes	69

Chapter 7	Accounts	71
	There are four pre-installed accounts	72
	How many people can use Network Discovery at once	72
	How the types of accounts differ.	72
	Creating accounts	74
Chapter 8	Backup and Restore	77
	About external backups	78
	Choosing tape or an FTP site for your external backup	79
	Configuring an external backup	79
	Testing your external backup and restore.	81
	To run an internal or external backup immediately	82
	Restoring your data	82
Chapter 9	To Upgrade from InfraTools Network Discovery	85
	How it works	86
	Configure your corporate firewall	86
	Upgrade the license on your new appliance	87
	Ensure that you have a backup from your old appliance	87
	Restore the old data to the new appliance.	87
	You can keep your IND Seeds, Blocks and Forces	88
Chapter 10	Before you call...	89
	Overview	90
	Check that your maintenance license is current	90
	Check that you have the latest software components	90
	Download the new components to your appliance	90
	Install the new component(s)	91
	After you install new components	91
Appendix A	Security Checklist	93
Appendix B	Extra Hardware	95
	Uninterruptible Power Supply (UPS) units	95
	Tape Drive	97
	External Modem	97

1

Welcome to Network Discovery

CHAPTER

Thank you for using Peregrine's Network Discovery! This book is intended for the Network Discovery Administrator, the person who will have the most control over the setup and operation of Network Discovery.

Topics in this chapter include:

- *Setup overview on page 6.*
- *Why it's important to do the preliminary work on page 6*
- *Collect information on page 7.*
- *Prepare the network on page 9.*
- *Check the management workstation on page 12.*

Overview

Peregrine's Network Discovery (PND) is a real-time web-based network manager. When integrated into your network, Network Discovery will discover and monitor all-SNMP-managed devices in your network. You will use Network Discovery to find, diagnose and solve network problems.

Important: If you are upgrading from InfraTools Network Discovery (IND) 4.2, 4.3, or 4.3.1, see chapter 9 *To Upgrade from InfraTools Network Discovery* on page 85.

Peregrine's Express Inventory (the WMI collector) can now contribute data to Network Discovery

Peregrine's Express Inventory (WMI) collector gathers information about Windows workstations using Windows Management Instrumentation (WMI). This WMI information can now be added to the Network Discovery database. References to scan files in the interface are to scan files that can be contributed by the Express Inventory (WMI) collector. For information on setting up and using the WMI Collector, see your ServiceCenter Essentials documentation.

Setup overview

Setting up Network Discovery is quick and easy, provided you properly prepare yourself, your network, and your management workstation.

There are three stages to setting up Network Discovery:

- Preliminary work: preparing your network devices
- Hardware setup: setting up the Peregrine appliance
- Software setup: configuring Network Discovery

Why it's important to do the preliminary work

To operate correctly, Network Discovery needs a constant supply of accurate information. To ensure that Network Discovery knows where and how to collect that information, you must do a little preliminary work. You only have to do this once.

The complete physical connectivity of your network can only be portrayed accurately when:

- all community strings are provided to Network Discovery
- all network connectivity devices are SNMP managed
- no network devices use proxy ARPing
- no critical entries appear in the Network Exceptions report

If devices do not conform to the standards or fail to respond correctly and consistently to SNMP polls, Network Discovery may not be able to create an accurate inventory.

Do the preliminary work properly. Trying to do it over, or postponing it until later, will be difficult and time-consuming. Just as there are three main parts to setting up Network Discovery so there are three main parts to the preliminary work:

- Collect information about your devices so that you can correctly configure Network Discovery
- Prepare the network devices for interaction with Network Discovery
- Check that the workstation you'll be using as a management console is properly equipped

Collect information

The *Pre-setup Questionnaire* is designed to help you gather information about your network. If you have already filled out this form, collecting all the information is done. Keep the completed questionnaire handy.

A review of the information on the *Pre-setup Questionnaire*

1. Assign an IP address for the Peregrine appliance.

You will need this IP address when preparing your network.

You will also need this IP address to perform basic configuration of your Peregrine appliance.

Note: If your network uses DHCP, ensure that the IP address for the Peregrine appliance is static.

Note: Record this IP address so that new users who are logging in can find it easily.

Note: Assign a domain name to the Peregrine appliance IP address. Record the domain name as well.

2. List ranges of IP addresses where devices might be found.

Network Discovery works best when you give it a broad idea of where the devices in your network are—but exclude ranges where you know there are no devices.

The *Pre-setup Questionnaire* asked you to list ranges of IP addresses where devices might be found.

Note: While you are making a list of devices in your networks, indicate bridges, routers, switches, and concentrators so that you can identify them easily. A list of bridges, routers, switches, and concentrators is essential in *Prepare the network*, step 1.

3. List community strings assigned to all devices.

A community string is like a password. Network Discovery must know at least one of a device's passwords to collect information from that device.

Note: Community strings are case-sensitive. “Public” and “public” are two different strings.

Note: Leave room on your list to include any community strings that will be created when you turn SNMP management on for devices.

This list is of non-directed community strings. Directed community strings are covered in step 3 of the next section, *Prepare the network*.

Troubleshooting - What happens if you don't give Network Discovery the community string for a device?

- Network Discovery will treat the device as though it does not have SNMP management turned on. You don't want that to happen.

Troubleshooting - Does Network Discovery need to know the write string?

- No. Network Discovery will operate without write strings. However, if you do give Network Discovery the write strings, admin accounts can fully manage a device right from the Network Discovery interface (see the *Network Discovery User Guide* for more information).

4. Check your Committed Information Rate (CIR) values

If your network uses Frame Relay, check your Committed Information Rate (CIR) values for your connectivity devices.

The CIR values for these devices are available from your service provider. Check the appropriate documentation to obtain these values.

Prepare the network

1. Turn on SNMP management in all switches and routers.

Important: You must do this first. Go no further until it is done.

Depending on the device, this may be a case of enabling an existing SNMP agent or setting up an SNMP agent.

You may also turn on SNMP management in other devices (see step 2). Often, the more managed devices in your network, the better. However, enable switches and routers first.

Note: If you use DHCP (Dynamic Host Configuration Protocol) in your network, set the IP address lease time to at least 7 days and turn on SNMP management on the DHCP servers.

Note: If you use HSRP (Hot Standby Routing Protocol) in your network, ensure you turn on SNMP management in all the affected devices.

When you turn on SNMP management in a device, you often assign a community string. If you assign a new string, be sure you add the string to your list of community strings.

Troubleshooting - What if I don't turn on SNMP management in my switches and routers?

- Network Discovery will appear to work, but you'll eventually notice that it appears to be working poorly, and you will need to complete the steps in *Prepare the network* all over again. Much of the information that Network Discovery collects comes from the SNMP MIB of devices in your network, so it is crucial that you do this, and do it now.

Troubleshooting - How do I do it?

- The exact procedure is different for every device. Consult the documentation that came with your switch or router.

2. (optional) Turn on SNMP management in hubs, servers, and workstations.

Whether you take this step depends on the results you expect from Network Discovery. In many networks, monitoring the performance of workstations is not important.

To improve the reliability and speed of Network Discovery, adjust bridge aging on your bridges, routers, switches, and concentrators. Turn bridge aging on, and set the bridge aging interval to 2-6 hours. Smaller networks can use shorter intervals; larger networks will need longer intervals.

3. Add the IP address of the Peregrine appliance to the list of all devices using directed community strings.

Community strings are like passwords for a device. Directed community strings provide devices with another layer of protection: a list of IP addresses of approved devices. When Network Discovery tries to get information from such a device, the device asks not only “What’s the password?” but also “Are you on the list?”

Note: Community strings are case-sensitive. “Public” and “public” are two different strings.

When directed community strings are used, it is not enough to configure Network Discovery to know how to access the device. You must also configure the device to know about the Peregrine appliance.

What happens if a device with directed community strings is not configured with the IP address of the Peregrine appliance?

- Network Discovery will treat the device as though it does not have SNMP management turned on. You don’t want that to happen.

4. Assign a device and port to which the Peregrine appliance will be attached.

Plan to attach the Peregrine appliance:

- to a device close to the top of your network
- behind your corporate firewall

Note: Attach a management workstation to the same device as the Peregrine appliance. This will make the setup process smoother. It will also ensure that the management workstation will not become isolated from Network Discovery in the event of device failures.

The port must be 10Base-T or 100Base-T. Network Discovery will automatically detect whether the port is 10 or 100, either full- or half-duplex. Network Discovery works best if the port is SNMP managed.

5. Allow access to Peregrine Systems Customer Support

For customer support by way of a modem, assign a dedicated telephone line for the Peregrine appliance.

Peregrine Systems will use this line for connection to the Peregrine appliance during its normal operation (not just during setup).

Note: Keep this line available for use by the Peregrine appliance 24 hours a day, 365 days a year. Peregrine Systems cannot provide you with modem support unless it has access to your Peregrine appliance.

For customer support by way of the Internet, configure the corporate firewall to allow the Peregrine Systems IP address 209.167.240.9 (sprocket.loran.com) to make inbound connections on the following ports:

- 22/tcp (SSH)
- 80/tcp (HTTP)
- 8100/tcp through 8105/tcp
- 8108/tcp

6. Configure the corporate firewall

If you have a corporate firewall that could impede Network Discovery from performing, configure the corporate firewall to allow ICMP (ping) to pass through, and enable the following ports:

- 22/tcp (SSH)
- 25/tcp (SMTP)
- 53/udp (DNS server)
- 80/tcp (HTTP)
- 123/udp (NTP server)
- 137/udp (NetBIOS)
- 161/udp (SNMP)
- 162/udp (SNMP-trap)
- 8100/tcp (MIB browser)
- 8101/tcp (Network Map)

- 8102/tcp (Network Map proxy)
- 8103/tcp (MIB Browser proxy)
- 8104/tcp (Telnet proxy)
- 8105/tcp (HTTP proxy)
- 8108/tcp (MySQL ODBC)
- 33263 (Traceroute)

Note: These are all standard ports; we list them here for your convenience.

7. Check Cisco devices

It is strongly recommended that firmware/software in your Cisco devices be IOS version 12 or higher. If you want ATM or Frame Relay support, IOS 12 is mandatory in your Cisco devices.

Check the management workstation

Because Network Discovery is web-based, you can use any properly equipped workstation as a management console.

Table 1-1: Requirements and recommendations for the management workstation s

Item	Required	Recommended
Web browser	Use Netscape 4.07 or later ^{ab} (but do not use 4.60 and do not use Netscape 6.x except 6.2.2 or later)	Netscape 4.7 or later
	Internet Explorer 5.0 or later ^c	Internet Explorer 5.0 or later
Video		
—colors	256 ^d	65,000 or more
—resolution	800×600	1024×768 or more
Memory (MB RAM)	32 ^e	64 ^f or more
CPU	Pentium 100 equivalent	Pentium II 233 equivalent or better

aNetscape 4.07 or later offers Y2K compliance.

bDo not use Netscape 6.x except for Netscape 6.2.2.

cRequires a Virtual Machine (VM) upgrade.

d256 colors normally give adequate performance. However, when using Netscape (with Windows 95, Windows 2000, or Windows NT), there may be unexpected colors on the Network Map.

eYou must close all applications other than your web browser.

f128 MB is recommended for large network maps.

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

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

Java Support

Earlier versions of Internet Explorer and Netscape required the use of the native Java environments. Alternate Java environments are now available, as follows:

Browser	Java Environment
Internet Explorer 5.0	Native only
Internet Explorer 5.5	Native or JRE 1.4
Internet Explorer 6.0	Native or JRE 1.4
Netscape 4.x	Native only
Netscape 6.2.3	JRE 1.4

2 | Install and Start Network Discovery

CHAPTER

This chapter describes how to install the hardware and how to start the Peregrine appliance for the first time.

Topics in this chapter include:

- *Install the hardware on page 16*
- *Connect the Peregrine appliance to the network on page 16*
- *Connect a keyboard and monitor or a terminal directly to the Peregrine appliance on page 17*
- *Connect data backup equipment and pager hardware on page 19*
- *Connect the Peregrine appliance to AC power on page 20*
- *Start Network Discovery the first time on page 20*

Install the hardware

If you have not already installed your Peregrine appliance, do so now, following the server installation documentation. The server installation documentation may vary depending on what version of server your Peregrine appliance is. The server installation documentation was included in the shipping box. If the documentation is missing or you have a problem, contact Peregrine Systems Customer Support.

Note: The Peregrine appliance comes with the software installed.

Connect the Peregrine appliance to the network

Attach the Peregrine appliance to a device close to the top of your network.

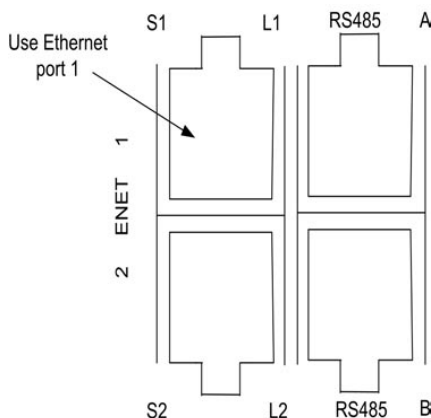
The device should be behind your corporate firewall.

Warning: Peregrine Systems strongly recommends that the Peregrine appliance be placed on the inside of the corporate firewall.

The port that allows the Peregrine appliance access to the network should be SNMP managed.

On the IBM xSeries server version of the Peregrine appliance, use ethernet port 1, the top left port, to connect the Peregrine appliance to the device close to the top of your network.

Figure 2-1: IBM xSeries server ports



Connect a keyboard and monitor or a terminal directly to the Peregrine appliance

You need equipment that communicates directly with the Peregrine appliance so that you can use the configuration interface to get Network Discovery up and running. The following instructions are for the IBM server xSeries version of the Peregrine appliance.

You have two options. Both are customer supplied; they do not ship with the Peregrine appliance:

- a keyboard and monitor
- a terminal or a workstation running terminal emulation software

To use a keyboard and monitor

- 1 Following the server installation documentation, connect the output end of the C2T breakout cable to the C2T (Out) connector on the back of the Peregrine appliance.
(The C2T breakout cable is packed in the C2T cable kit.)
- 2 Connect the keyboard and monitor ends of the cable to the keyboard and monitor.

- To use a terminal or a workstation running terminal emulation software
- 1 Connect the terminal or workstation to the Serial connector on the Peregrine appliance.
 - 2 If you are using terminal emulation software, start the program. (For example, in Windows, **Start > Programs > Accessories > Communications > HyperTerminal**).
 - 3 The terminal must meet the following requirements or, if you are using terminal emulation software, use the following settings.

Table 2-2: Terminal requirements or settings

Item	Requirement
Speed	9600
Bits	8
Parity	None
Stop Bits	1
Terminal type	vt100

Connect a management workstation to the network

You will use the management workstation to use the browser interface once Network Discovery is up and running.

Connect your management workstation to the network. Even though you can connect your management workstation anywhere, we recommend that you connect a dedicated management workstation to the same concentrator or switch as the Peregrine appliance. When you are starting up, having a management workstation close to the Peregrine appliance makes it easier for you to check for loose connections and avoids problems due to network partitions.

Connect an Uninterruptible Power Supply (UPS)

Connecting an uninterruptible power supply (UPS) is optional. For information about UPS units that will work with the Peregrine appliance, see *Appendix B, Extra Hardware* on page 95.

Warning: If Network Discovery does not detect a UPS, it will issue a constant warning about the health of the Peregrine appliance.

Note: If you wish to disable the warning, see *About disabling UPS and backup warnings* on page 43.

Connect data backup equipment and pager hardware

Connecting data backup equipment is optional. Connecting pager hardware is also optional.

If you choose to connect an external modem for paging or a tape drive for data backup, you should do so now. For more information on paging, see the *Network Discovery User Guide*. For more information on backing up and restoring data, see *Backup and Restore* on page 77.

For tape drive requirements, see *Appendix B, Extra Hardware* on page 95.

Installing data backup equipment and pager hardware are the responsibility of the customer. If you have any problems, contact Peregrine Systems Customer Support.

Note: You can add a tape drive later, after Network Discovery is up and running. You will not have to restart the Peregrine appliance. However, after Network Discovery has been running, if you unplug the tape drive and plug it in again, the tape drive will lock. To unlock it, you must restart the Peregrine appliance.

Note: It is also possible to back up data without a tape drive by using an FTP server instead.

Connect the Peregrine appliance to a telephone line

Connecting the Peregrine appliance to a telephone line is optional.

The Peregrine appliance is equipped with an internal modem to enable connection to a standard analog telephone line. This connection allows Customer Support to perform remote diagnostics and software upgrades.

To connect the Peregrine appliance to a telephone line

- 1 Plug one end of a telephone line cable into the modem connector on the back of the Peregrine appliance.
- 2 Plug the other end of the cable into a standard telephone line connector.
- 3 Record the telephone number of this line for future use.

Note: Keep this line available for use by the Peregrine appliance 24 hours a day, 365 days a year. Peregrine Systems cannot provide you with support unless it has access to your Peregrine appliance.

Connect the Peregrine appliance to AC power

Follow your server installation documentation to connect the AC power and turn the server on.

Start Network Discovery the first time

The configuration interface—available through a terminal or a monitor and keyboard connected directly to the Peregrine appliance—is used when you cannot access Network Discovery by means of your web browser. Working with the configuration interface, you will enter the IP address of the Peregrine appliance, the network mask (also called a netmask), and the IP address of the gateway. This information is on your completed *Pre-setup Questionnaire*. Until the information is entered, the Peregrine appliance will not collect data from the network.

To log in to the Network Discovery through the configuration interface

On the terminal or monitor connected directly to the Peregrine appliance, the screen shows:

Press Enter to access the Configuration menu.

- 1 Press **Enter**.

The screen shows:
Password

- 2 Type **Appliance**

The “A” is uppercase.

To use the configuration interface to get Network Discovery up and running

The screen shows

- 1) Settings
- 2) Actions
- 3) System Configuration
- 4) Exit and Log off

1 Type 1 (or use the arrow keys to move the cursor to 1)

2 Press **Enter**.

The screen shows

- 1) Return to main menu.
- 2) IP Networking
- 3) Appliance system variables
- 4) Appliance community strings
- 5) Host name
- 6) Workgroup
- 7) Administrator's E-mail Address
- 8) Mail server
- 9) Time server
- 10) Change password

3 Type 2

4 Press **Enter**

The screen shows:

- 1) Return to main menu.
- 2) Refresh
- 3) IP ADDRESS
- 4) NETMASK
- 5) GATEWAY

5 Type 3

6 Press **Enter**

7 Type the IP address of the Network Discovery appliance.

8 Press **Enter**

Repeat steps 5 to 8 to enter the netmask and gateway

Note: If your network has no gateway address, enter the IP address of the Network Discovery appliance for the gateway.

The screen shows the menu again, but with the addition of **6) Submit changes**.

9 Type **6**

10 Press **Enter**

11 Wait briefly.

Now you will be able to access Network Discovery through your web browser.

12 Type **1** to return to the main menu.

13 Type **4** to exit and log off.

3 Appliance Management

CHAPTER

Some of the tasks in this chapter are optional.

Topics in this chapter include:

- *Log in to Network Discovery on page 24*
- *How to shut down the Peregrine appliance on page 27*
- *The Home page on page 28*
- *The Toolbar on page 29*
- *Assign a system name, contact, and location on page 31*
- *Change the Peregrine appliance community strings on page 32*
- *Set the time zone on page 33*
- *Enter the domain name server on page 34*
- *Enter the host name on page 35*
- *Enter the Workgroup name on page 36*
- *Enter the Administrator e-mail address on page 37*
- *Enter the SMTP server on page 38*
- *Set the system time on page 39*
- *Change the default Admin password on page 41*
- *About disabling UPS and backup warnings on page 43*

Log in to Network Discovery

To log in to Network Discovery, you must have the following:

- access to a web browser
- a browser with Java and JavaScript turned on
- the IP address or domain name of the Peregrine appliance
- a valid Network Discovery account name and password

Network Discovery is shipped with four pre-defined accounts.

Table 3-3: The four types of accounts with their default passwords

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

For your first session with Network Discovery, you should use the account named “admin.”

To log in to Network Discovery

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

When the connection is made, the Network Discovery splash screen and Login window appear.

Note: You can bookmark this URL for use with your browser.

- 3 Enter the default account name (“admin”) and password (“password”).

Note: Account names are all lower case.

Passwords are case-sensitive. “PASSWORD” and “password” are two different passwords.

- Once the account name and password are accepted, the Network Discovery Home page and Toolbar appear.

- After the Toolbar appears, but before it is activated for use, Internet Explorer or Netscape (version 6.0 or greater) displays a security warning. You are asked to grant Network Discovery permission to run.

4 Click Yes.

To avoid being asked this question again

- ▶ Click the check box next to “Always trust content from Peregrine Systems Customer Support, Inc.”

Note: This should be the only time you use the default password for the “admin” account. See *Change the default Admin password* on page 41.

Before you begin setting up the Network Discovery software, you’ll need a brief introduction to the Home page and the Toolbar.

Troubleshooting when logging in for the first time

Why can’t I connect to Network Discovery?

- If you entered the correct URL in your browser, it is likely that the IP address, network mask, or gateway address were not entered correctly when you started Network Discovery the first time (*Start Network Discovery the first time* on page 20). You can go back and check in the startup procedure at the equipment connected to the Network Discovery appliance.
- If the configuration information is correct, it may be that your management workstation cannot reach that portion of the network to which the Peregrine appliance is connected. It is recommended that the workstation or laptop used as your management console be connected to the same concentrator, switch, or router as the Peregrine appliance, at least during your first use of Network Discovery.
- Try pinging the IP address of your Peregrine appliance. If the Peregrine appliance does not respond, try pinging the concentrator or switch to which the Peregrine appliance is attached. If the concentrator or switch also does not respond, the problem is probably not with the Peregrine appliance.
- Double check that the link light on the back of the Peregrine appliance is lit. If this light is not lit, you will not be able to connect to your Peregrine appliance.

I can access the web page, but it shows me a startup log rather than the Network Discovery splash screen.

- Your Peregrine appliance is not yet ready for you to log in. Please, wait. If the problem persists, call Peregrine Systems Customer Support.

It's still not working; what should I do?

- If the Peregrine appliance fails to respond, contact your Peregrine Systems Customer Support representative for further assistance.

The Login did not appear.

- Click the Network Discovery splash screen.

The Toolbar did not appear.

- Your browser has JavaScript turned off.

The Toolbar appeared, but the status window is blank.

- Your browser has Java turned off.

I can connect to the Peregrine appliance, but I cannot open a component I would expect to see with my license, such as the Network Map or ODBC. The two most common reasons for this problem are:

- Your management workstation and the Peregrine appliance are on opposite sides of your corporate firewall. You should see a dialog box that explains that Network Discovery is trying to connect and shows an error message.

To resolve the problem, do one of the following:

- Ensure that your management workstation and the Peregrine appliance are on the same side of the firewall.
- Configure the firewall to allow connections from the subnet with your management workstation to the subnet with the Peregrine appliance for the ports: 80, 8100, 8101 to 8105, and 8108.
- Your web browser may be configured to use a proxy server.

To resolve the problem:

- If you have a manual proxy connection, you may be able to add your own exception or bypass.
- If you have an automatic proxy connection, it may be necessary to consult the administrator for your network.

How to shut 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.

Warning: Do not shut down the Network Discovery appliance during the startup procedure unless you need to abandon the startup procedure.

To shut down the Peregrine appliance safely, follow one of these two procedures.

To shut down the Peregrine appliance (through the browser interface)

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

The Peregrine appliance shuts down safely.

To shut down the Peregrine appliance (through the configuration interface)

The main menu shows:

- 1) Settings
 - 2) Actions
 - 3) System Configuration
 - 4) Exit and log off
- 1 Type 2
- The screen shows
- 1) Return to main menu.
 - 2) Appliance shutdown
 - 3) Appliance restart
 - 4) Set time
 - 5) Synchronize time
 - 6) Add licenses

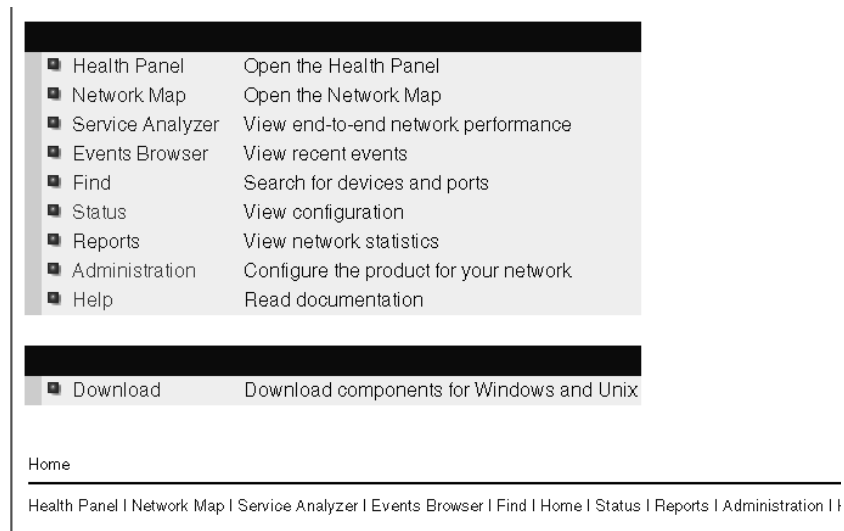
- 7) Check CD
- 2 Type 2
 - The screen shows:
 - 1) Return to main menu.
 - 2) Shut down the appliance
- 3 Type 2
 - The Peregrine appliance shuts down safely.

The Home page

The Home page welcomes you to Network Discovery. On the Home page, you will see links to the major features of Network Discovery, each with a brief description.

Because the Home page is the first page that you see after logging in to Network Discovery, the Home page also serves as an introduction to the navigation hyperlinks. The navigation hyperlinks appear at the bottom of the Home page (as well as at the bottom of the Report, Status, Administration, and Help windows).

Figure 3-2: Home page



The first row of hyperlinks (which sometimes ends in plain, unlinked text) shows you the path you have followed in the menus. These hyperlinks help you to visualize where you are in the menus, and help you to get back to where you started.

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

The Toolbar

The Toolbar provides a way to navigate through Network Discovery. The Toolbar has three main parts:

- banner or title bar
- buttons
- status window

Figure 3-3: Toolbar















The banner or title bar

The Toolbar banner displays the system name. Because you have not yet assigned a name, the banner displays “Unknown.”

The buttons

There are three groups of Toolbar buttons. Some buttons may be unavailable, depending on your license.

The first group of buttons contains the major functions of Network Discovery.	
	Health Panel—opens the Health Panel.
	Network Map—opens the Main Map to show you how your network looks right now.
	Service Analyzer – allows you to view and evaluate a path between two network devices.
	Events—opens the Events Browser to show you events that have taken place in the last 45 days.
	Find—finds and focuses on a specific device.
The second group of buttons uses the active browser window.	
	Home—provides a brief guide on how to get started with Network Discovery; also the first screen you see when logging in.
	Status—displays information on the Peregrine appliance itself, and how it is functioning.
	Reports—displays a variety of reports about your network as a whole and about specific devices and groups of devices.
	Administration—the function of this button depends on your account.
	Help—displays the manuals, release notes, and other information.
The third group of buttons controls exiting—whether you will close Network Discovery windows or close Network Discovery completely.	
	Close all windows—unclutters your desktop by closing all opened Network Discovery windows.
	Exit—quits Network Discovery completely (but leaves your web browser active).

The status window

The status window displays three types of messages:

- The version/user message appears, and details the version of Network Discovery, and the full name for your account.
- Mini-help messages appear when you point to a Toolbar button.
- Map-loading progress messages appear when Network Discovery is loading the Main Map and the Health Panel.

Assign a system name, contact, and location

The system name is the name of the network or part of the network that Network Discovery is currently managing. The system name is displayed in the Toolbar banner.

“System contact” is the person who will receive e-mail from Network Discovery (assuming Network Discovery is set up to send e-mail). “System location” is the physical location of the Peregrine appliance. These are standard SNMP entries; assign them according to your corporate policy.

To assign a system name, contact and location

- 1 Click **Administration > Appliance Management > Appliance System Variables**.
- 2 Enter the system name.
The system name can be a maximum of 200 characters long (including spaces)
- 3 Enter the system contact.
- 4 Enter the system location.
- 5 Click **Change**.

Note: The new system name does not appear in Toolbar banner until you close and reopen the Toolbar.

Change the Peregrine appliance community strings

You can change the following community strings on this screen:

- read-only community string (used to allow read access to the Peregrine appliance MIB).
- read/write community string (used to allow read and write access to the Peregrine appliance MIB).

We recommend you do the following:

- Do not change the read-only community string; or, change the read-only string to the one used by the rest of the devices in your network.
- Do change the read/write community string (for security reasons).

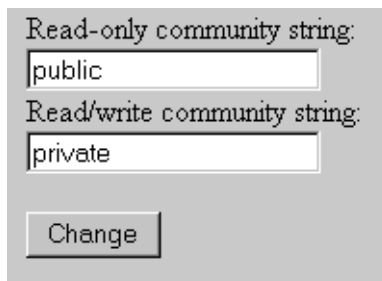
Note: Community strings are case-sensitive. “PUBLIC” and “public” are two different strings.

Note: For information on community strings, see *About community strings* on page 52 and *More on community strings* on page 66.

To change the Peregrine appliance community strings

- 1 Click **Administration > Appliance management > Appliance community strings**.
- 2 Type the new read-only or read/write community string in the appropriate field.
- 3 Click **Change**.

Figure 3-4: Change community strings



Read-only community string:
public

Read/write community string:
private

Change

Set the time zone

Note: You must set the time zone when first configuring Network Discovery.

Changing to the appropriate time zone will allow Network Discovery to adjust the local time relative to Coordinated Universal Time. Network Discovery will also calculate daylight savings time automatically as appropriate.

The default time zone is Canada/Eastern.

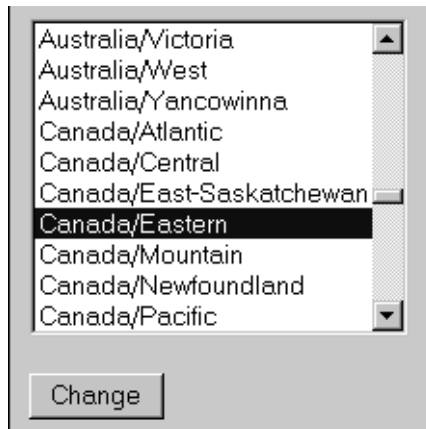
Warning: The time zone must be set when the Peregrine appliance is first set up. If the time zone has not been set, or if you change the time zone, the Network Map may not be updated for a period equal to the difference between the two time zones.

To change the time zone

- 1 Click **Administration > Appliance management > Time zone**.
- 2 Select the correct time zone from the scroll list.
- 3 Click **Change**.

Note: When you change the time zone, some software modules restart and you may see a Start Log message. This is normal. Network Discovery may not be available for a couple of minutes. (If you change it later, when there is more data, Network Discovery could be unavailable for 5 to 10 minutes.)

Figure 3-5: Changing the time zone



Enter the domain name server

A domain name server translates between alphabetic domain names—also known as DNS names—(for example, “website.example.com”) and numeric IP addresses (for example, “192.168.133.1”). Network Discovery needs to know where your domain name servers are so that it can take advantage of this “translation service.”

Unless you set the domain name server, domain name will not appear on map windows, in reports, and so on.

You can change the following elements in this window:

- domain name server
- domain search order

To enter the domain name server

- 1 Click **Administration > Appliance management > Domain name servers**.
- 2 Type the IP address (IPv4) of the new domain name server in the top field. To enter more than one, separate each IP address with a comma (no space).
- 3 Click **Change**.

To enter the domain search order

- 1 Click **Administration > Appliance management > Domain name servers**.

- 2 Type the new domain search order in the bottom field.

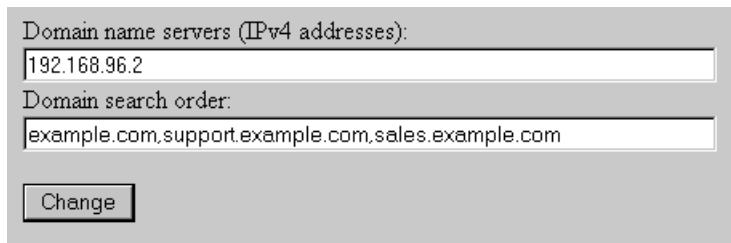
When you enter the domain names in the domain search order field, separate the entries with commas (no spaces). For example, “example.com,eastern.example.com,sales.example.com”.

Default domains are used to extend domain names so that it is possible to enter domain names in a shorter form. For example, if you enter a domain name as “loman”, Network Discovery will first try to complete the name as “loman.example.com”, then “loman.eastern.example.com”, then “loman.sales.example.com”.

- 3 Click **Change**.

Important: Network Discovery will automatically restart several processes after changing the domain name servers. Network Discovery will not respond for a short period after you click **Change**. This is normal.

Figure 3-6: Change domain name server



Domain name servers (IPv4 addresses):
192.168.96.2

Domain search order:
example.com,support.example.com,sales.example.com

Change

Enter the host name

A host name allows you to refer to a device by a name rather than an IP address. Network Discovery uses the host name to refer to itself in the e-mails it sends.

Note: Define a domain name server before changing the host name.

The **Host name** page has two modes: prompted and manual.

In prompted mode, Network Discovery will try to read its own host name from the domain name server. If Network Discovery finds a host name matching its IP address, you will be asked to confirm that the match is correct.

In manual mode, Network Discovery has failed to find a match for its own IP address. You will be given the option to enter a host name.

To change the host name

- 1 Click **Administration > Appliance management > Host name**.
 - If the Current host name is correct, click **Confirm**. No further action is necessary.
 - If you want to change the Host name, go to step 2.
- 2 Enter the new host name.
- 3 Click **Change**.

Figure 3-7: Change host name



nmserver.example.com

-or-

Host name:

Enter the Workgroup name

Enables you to change the NetBIOS workgroup name. Workgroups are used primarily by Microsoft Windows. The workgroup name determines where in your Network Neighborhood you will find the Peregrine appliance.

The Peregrine appliance has an SMB shared directory into which you can deposit:

- license files when you download them from the Peregrine Customer Support web site
- scan files from Express Inventory (the WMI collector)

The current workgroup name is shown below. The default name is WORKGROUP.

The workgroup name must be 0-15 characters long. The name may contain only alphanumeric characters (A-Z, a-z, 0-9), hyphen (-) and period (.). Spaces are not permitted.

To enter the workgroup name

- 1 Click **Administration > Appliance Management > Workgroup**
- 2 Type the workgroup name.
- 3 Click **Change**.

Enter the Administrator e-mail address

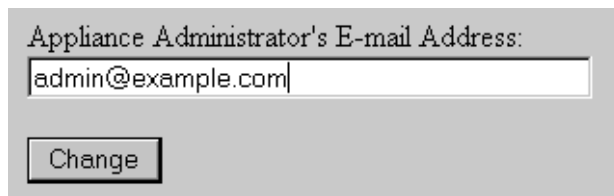
Enter the e-mail address of the Network Discovery Administrator, and that address will receive information on mail delivery problems.

Warning: If you do not supply an e-mail address, no mail will be sent, even if a mail server is indicated on the **SMTP Server** page.

If you enter an e-mail address that is not valid, you will cause “message undeliverable” e-mails to be sent to the account of the administrator for the mail server. This account is normally called “postmaster”. Consult your mail server’s documentation for details.

To enter the Network Discovery Administrator e-mail address

- 1 Click **Administration > Appliance management > Appliance administrator e-mail address**.
- 2 Enter the e-mail address of the Network Discovery Administrator.
- 3 Click **Change**.

Figure 3-8: Enter e-mail address

Appliance Administrator's E-mail Address:
admin@example.com
Change

Enter the SMTP server

Entering an SMTP server is optional.

An SMTP server handles standard Internet e-mail. Network Discovery can use this server when it generates e-mail messages to tell you what is going on in your network or with other processes such as a daily backup.

If you do not enter an SMTP server, e-mail from Network Discovery will go to the default mail server for the domain. You may prefer to specify an SMTP server because the e-mail will go faster routed through a local server.

The SMTP server can be on-site or off-site (that is, part of your own network or part of another network). However, if your mail server is off-site, you may not be able to rely on it to send you a message that a network device is down. A local SMTP server or paging (if you have an Network Discovery license) are recommended.

Note: Setting up the SMTP server and supplying an e-mail address are two separate tasks. If you do not supply an Network Discovery Administrator e-mail address, no mail will be sent, even if a mail server is indicated on the SMTP Server page.

To enter the SMTP server

- 1 Click **Administration > Appliance management > SMTP server**.
- 2 Enter the Host name or IPv4 address of the SMTP server.
- 3 Click **Change**.

Figure 3-9: Change SMTP server



Host name or IPv4 address:
mail.example.com

Change

Set the system time

This time is used by Network Discovery to monitor your network, to generate reports, and to track daylight savings time (where appropriate).

Perform one of the two following procedures, not both.

- *Set the date and time*, next section
- *Synchronize the time* on page 40 (or *Enter an NTP server to synchronize the time (continually)* on page 41)

Set the date and time

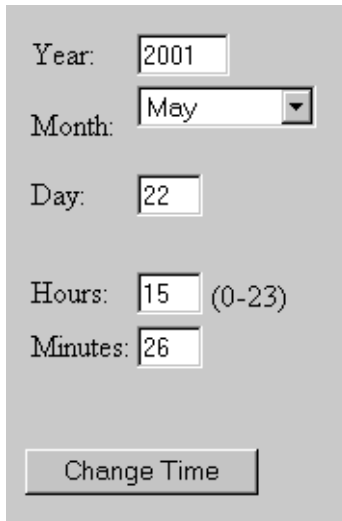
Note: The “Hours” field uses the 24-hour clock, so times between noon and midnight must be specified as being between 12:00 and 23:59. For example, 3:45 PM is specified 15:45.

Note: Seconds are not set explicitly. When you click the Set Time button, seconds are set to 0.

To set the time and date

- 1 Make sure the time zone is set (see *Setting the time and date* on page 40).
- 2 Click **Administration > Appliance management > Set time**.
- 3 Enter the Year, Month, Day, Hours, and Minutes in the appropriate fields.
- 4 Click **Change Time**.

Figure 3-10: Setting the time and date



Year:

Month:

Day:

Hours: (0-23)

Minutes:

Synchronize the time

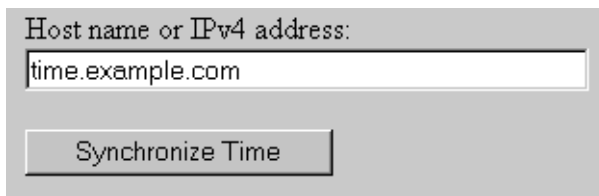
This procedure synchronizes the time used by Network Discovery with the time on another machine that uses the Network Time Protocol (NTP).

Either set the time or synchronize the time, not both.

Note: The Synchronize Time option only synchronizes the time once. It does not repeatedly re-synchronize.

To synchronize the time

- 1 Make sure the time zone is set (see *Setting the time and date* on page 40).
- 2 Click **Administration > Appliance management > Synchronize time**.
- 3 Enter the IPv4 address of the server with which you want to synchronize time.
- 4 Click **Synchronize Time**.

Figure 3-11: Synchronize timeA screenshot of a web interface dialog box. At the top, it says "Host name or IPv4 address:". Below this is a text input field containing "time.example.com". At the bottom of the dialog is a button labeled "Synchronize Time".

Host name or IPv4 address:
time.example.com
Synchronize Time

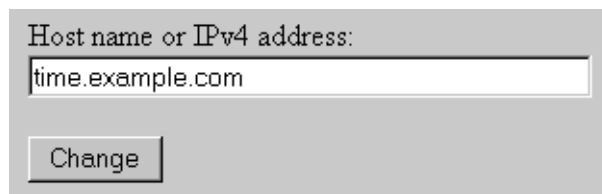
Enter an NTP server to synchronize the time (continually)

Entering an NTP server is optional.

An NTP (Network Time Protocol) server is a server that keeps track of and reports the exact time. Network Discovery can synchronize its system time with the time reported by the NTP server.

To enter the NTP server

- 1 Click **Administration > Appliance management > NTP server**.
- 2 Enter the Host name or IPv4 address.
- 3 Click **Change**.

Figure 3-12: Change NTP serverA screenshot of a web interface dialog box. At the top, it says "Host name or IPv4 address:". Below this is a text input field containing "time.example.com". At the bottom of the dialog is a button labeled "Change".

Host name or IPv4 address:
time.example.com
Change

Change the default Admin password

Once you have successfully logged in, you must do some administration of Network Discovery.

Note: You should change the password for the default admin account as soon as possible for security reasons. For additional security suggestions, see *Security Checklist* on page 93.

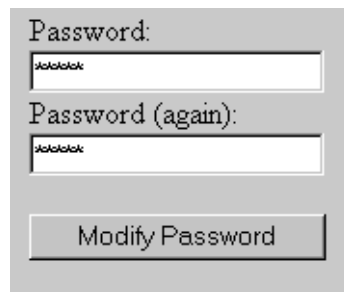
Note: When you change the password for the admin account, you will have to log in again. (It is always necessary to log in again when you change the password for the account you are using.)

Passwords can be 4–20 characters long. The password may contain upper and lower case letters (A–Z and a–z), numerals (0–9), underscores (_), hyphens (-), at signs (@), and periods (.

To change the admin 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**.

Figure 3-13: Changing the admin password

A screenshot of a web form for changing a password. It features two text input fields, one labeled "Password:" and the other "Password (again):", both containing masked characters. Below the fields is a button labeled "Modify Password".

Troubleshooting when changing your password

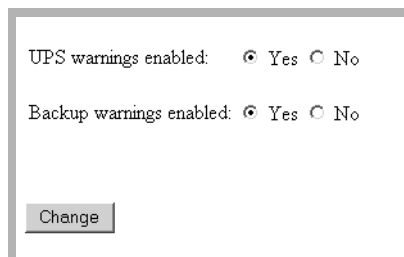
There was an error when I changed the password.

- ▶ Network Discovery will identify the error type. Your account will continue to use the old password. Contact Peregrine Systems Customer Support.

About disabling UPS and backup warnings

The use of a UPS (Uninterruptible Power Supply) and regular backups of Network Discovery data are both highly recommended. Network Discovery generates warnings if it does not detect a UPS or if daily backups have been configured but are not occurring. You can, however, choose to turn these warnings off.

Figure 3-14: Enable or disable UPS and backup warnings



The screenshot shows a dialog box with two radio button options. The first option is "UPS warnings enabled:" with "Yes" selected (indicated by a filled radio button) and "No" unselected (indicated by an empty radio button). The second option is "Backup warnings enabled:" with "Yes" selected (indicated by a filled radio button) and "No" unselected (indicated by an empty radio button). At the bottom of the dialog box is a "Change" button.

Disable the UPS warning

Note: Use this procedure only if you are not using an uninterruptible power source (UPS) with your Peregrine appliance.

This procedure controls whether Network Discovery generates a warning when a UPS is not detected.

We strongly recommend the use of a UPS (Uninterruptible Power Supply) with your Peregrine appliance. For that reason, if Network Discovery detects that no UPS is present, Network Discovery creates a warning condition for Appliance Health. The default is to have a warning.

If you will not be connecting a UPS directly to your Peregrine appliance, you may choose to have Network Discovery suppress this warning.

To enable or disable the UPS warning

- 1 Click **Administration > Appliance Services > Display warnings**
- 2 For UPS warnings enabled, click **Yes** or click **No**.
- 3 Click **Change**.

Disable the backup warning

We strongly recommend that you configure a backup of your Network Discovery data. For that reason, if Network Discovery detects that you have configured a backup and detects that it has not successfully completed a backup within the past 25 hours, Network Discovery will create a warning condition for *Appliance Health*.

If you have not configured a backup, you will not receive a warning. The default is Yes. You can turn this warning off.

To enable or disable the backup warning

- 1 Click **Administration > Appliance Services > Display warnings**
- 2 For Backup warnings enabled, click **Yes** or click **No**.
- 3 Click **Change**.

4 Licenses

CHAPTER

Peregrine continually improves Network Discovery with new software components to handle the new devices on the market and in your network. Because Network Discovery is on an appliance, it's easy for you to upgrade it with increased functionality and the latest software.

Topics in this chapter include:

- *How it works* on page 46
- *Request a new license* on page 46
- *Install the new license* on page 47

How it works

You request a license upgrade from Peregrine Systems, directly through Network Discovery. Then you receive the license file through e-mail and install it.

When you receive the Peregrine appliance, it has a default license on it. The license gives you:

- capacity for one map session at a time
- the ability to find ten devices on the network
- the ability to have ten resource-managed devices

You can use Network Discovery with this default license temporarily, or you can go ahead and request the license that will give you the full functionality you purchased, as well as the most up-to-date software components.

Note: To see what licenses are currently installed on your Peregrine appliance, see **Status > Current Settings > Installed Licenses**.

Note: To see what software components are currently installed on your Peregrine appliance, see **Status > Current Settings > Installed Components**

Request a new license

To request a license through Network Discovery

- 1 **Administration > Appliance Management > Generate licensing request.**
- 2 Complete the form.
- 3 If your Peregrine appliance is configured to send e-mail (the instructions were in chapter 3, *Appliance Management* on page 23), click **Send e-mail from the appliance to support@peregrine.com**

If your Peregrine appliance is not configured to send e-mail, click **Print out all the information, and I will e-mail it to support.**

- 4 Click **Generate Request.**

If you clicked **Send e-mail from the appliance to support@peregrine.com**, Network Discovery sends your request to Peregrine Systems Customer Support automatically.

- 5 If you clicked **Print out all the information, and I will e-mail it to support**, your request appears in printable format. Copy and paste the request into an e-mail and send the e-mail to support@peregrine.com

In either case, Peregrine Systems Customer Support responds with a confirmation that your request has been received and will be processed shortly.

Install the new license

Peregrine Systems Customer Support generates your new license file and sends it to you attached to an e-mail.

To install the new license

- 1 From the Windows **Start** menus, click **Run**.
- 2 Type `\\<appliance IP>\share\license\incoming`
(where `<appliance IP>` is the IPv4 address of your Peregrine appliance).
- 3 If you are asked to supply a user name and password, use the user name and password you use to log in to Network Discovery.
- 4 Drag and drop the new license file into the above directory.

Network Discovery finds the new file and verifies it. Then it performs the upgrade automatically and moves the license file to the shared directory, `\\<appliance IP>\share\license\processed`.

Note: If the component is not appropriate for installation, Network Discovery does not perform the upgrade and moves the file to the shared directory, `\\<appliance IP>\share\license\bad`.

Note: If the license asks the Peregrine appliance to do too much, (for example, a license for more devices than the Peregrine appliance can support) the Peregrine appliance will take the maximum it can do.

Note: To see what licenses are currently installed on your Peregrine appliance, see **Status > Current Settings > Installed Licenses**.

If you wish to upgrade from an InfraTools appliance, turn now to the procedures in chapter 9, *To Upgrade from InfraTools Network Discovery* on page 85 and come back to the next chapter when you are instructed to do so.

5 Set up Network Discovery

CHAPTER

Important: If you are upgrading from InfraTools Network Discovery (IND) 4.2.x or 4.3.x, or from Xanadu 1.0.4, follow the *To Upgrade from InfraTools Network Discovery* on page 85. This chapter does not include any upgrade information.

Network Discovery allows you to define quite precisely what devices in your network it will discover and how. For now though, keep things simple and set up Network Discovery to perform active discovery on all of the network that you know has devices.

Topics in this chapter include:

- *How it works* on page 50
- *Set up the IPv4 range(s) to discover* on page 50
- *Set up the IPv4 range(s) to avoid* on page 52
- *About community strings* on page 52
- *Activate your proposed changes* on page 53

How it works

Essentially, network configuration works as follows. You add IPv4 ranges that you want Network Discovery to monitor. Then you enter pieces of those IPv4 ranges that you want to be monitored differently or not at all. To the various pieces of IPv4 ranges you apply groups of properties (for example, “Do not allow discovery” or “Resource manage”). You can apply default groups of properties or customize your own. Network Discovery guides you with graphic views of the ranges you set up. The setup can be quite sophisticated. There is more information on how to take advantage of this flexibility in the next chapter, *Refining Network Discovery* on page 55.

For now though, to just get Network Discovery going, you don’t have to do much.

Set up the IPv4 range(s) to discover

Warning: If you want to keep your old style IND network configuration, do not activate changes to the new style of network configuration. Do not use the procedures in this section. For more information on how to upgrade from InfraTools Network Discovery, see *To Upgrade from InfraTools Network Discovery* on page 85.

View an IPv4 range

As soon as you entered the IPv4 address of the Peregrine appliance, Network Discovery automatically made a guess as to the subnet in which the Peregrine appliance resides. It may have made the right guess, or it may have suggested a range that is either too big or too small. Take a look at the suggested IPv4 range.

To view IPv4 ranges

- ▶ Click **Administration > Network configuration > List IPv4 ranges**.

If the IPv4 range suggested by Network Discovery is too big or too small, delete it and add the correct range or ranges. The IPv4 ranges for your network are on the *Pre-setup Questionnaire*.

Delete an IPv4 range

Do not remove or change the range, 0.0.0.0.–255.255.255.255.

To delete an IPv4 range

1 From **Administration** > **Network configuration** > **List IPv4 ranges**.

2 Select the IPv4 range.

If the range has subranges, Network Discovery gives you a choice of deleting only the range or of deleting the range plus all of its subranges.

3 Click **Delete this IPv4 range**.

4 Click **Delete**.

You have deleted the range in your proposed new configuration, but your change will not take effect until after you have reviewed and activated your changes.

Add an IPv4 range

For each subnet in your network that you want Network Discovery to discover, add a new IPv4 range.

To add a range of IPv4 addresses

1 Click **Administration** > **Network configuration** > **Add IPv4 range**.

2 Enter the starting and ending IPv4 addresses of your whole network or of a range in your network.

3 For **Property Set/Group**, select **Network: Active Discovery**.

Network Discovery will perform network discovery (ping, poll, and table read) on the range you have entered.

4 Click **Submit**.

Repeat steps 1 to 4, if necessary, for all your subnets.

You have added the range(s) to discover to your proposed new configuration, but your changes will not take effect until after you have reviewed and activated your changes.

Set up the IPv4 range(s) to avoid

Within an IP range that you have added, there may be an IPv4 range that your network does not use. For each subnet in your network that you want Network Discovery to avoid, add a new IPv4 range.

To add a range of IPv4 addresses

- 1 Click **Administration > Network configuration > Add IPv4 range**.
- 2 Enter the starting and ending IPv4 addresses for your network.
- 3 For **Property Set/Group**, select **Network: Do not allow discovery**.
Network Discovery will not perform network discovery on this IPv4 range.
- 4 Click **Submit**.

Repeat steps 1 to 5, if necessary, for all the subnets you want Network Discovery to avoid.

You have added the range(s) to avoid to your proposed new configuration, but your changes will not take effect until after you have reviewed and activated your changes.

About community strings

If all of your devices have the community string, “public”, you don’t need to read this section or add any community strings.

Community strings are a kind of password assigned to a device. Each device with a community string protects its SNMP MIB by asking every other device for the password before permitting its own MIB to be read from or written to. Because Network Discovery will attempt to communicate with all of the devices in the range(s) you have set up, Network Discovery must have community strings for all of the SNMP manageable devices. If Network Discovery doesn’t have the community strings, it can’t perform network discovery.

It works as follows. You give community strings to a Community Property Group and then apply the Community Property Group to an IPv4 range.

For now, just add all your community strings to one Property Group, the “global” Community Property Group.

Note: Community strings are case-sensitive. “PUBLIC” and “public” are two different strings.

To add community strings to the global Community Property Group

- 1 Click **Administration > Network Configuration > Community Property Groups**.
- 2 Click **Modify a Community Property Group**.
- 3 Select **Community: global** from the pull-down list.
- 4 Click **Select**.
- 5 Under the heading **Add a Community String** enter a string name, and select the appropriate **Type** (**read** or **write**, or both).
When you add community strings, the order is important, enter the most frequently used strings first.
- 6 Click **Add**.
- 7 Repeat steps 5 and 6 for each of your community strings.
- 8 If necessary, select a community string and click the **Move Up** or **Move Down** buttons to move it to the right place. Put the most frequently used community strings first.
- 9 Click **Submit**.

Note: To assign different community strings to different IPv4 ranges, see the next chapter, *Refining Network Discovery* on page 55.

Activate your proposed changes

The **Activate Changes** page allows you to review all the changes you have proposed for Network Discovery network configuration before actually making those changes take effect.

Note: Changes to network configuration do not take effect if you do not activate them.

To activate changes

- 1 Click **Administration > Network configuration > Activate Changes**.
A table appears, detailing all the changes made in this session.
Network Discovery tells you how many potential devices it will have to explore, and how long it will take.

Also, you will be told of any configuration problems detected by Network Discovery. You can ignore the warnings, but do so at your own risk.

- 2 Review the changes to make sure the new configuration is correct.

If you decide to implement the changes you have made, activating the changes will update your network configuration.

- 3 Click **Activate changes**.

All of the changes you proposed are now the current settings and Network Discovery will perform active discovery on the IPv4 ranges you have set up.

To check that network discovery is occurring

- 1 **Status > Appliance Health > Software Environment**
- 2 See if the number of discovered devices is increasing.
- 3 Open a Network Map. Devices should appear on your map within ten minutes.

6 Refining Network Discovery

CHAPTER

The procedures in this chapter are optional. You may wish to come back to this chapter after Network Discovery has been up and running for a while. Here you will learn how to take advantage of the precision Network Discovery offers you for setting up Network Discovery.

Topics in this chapter include:

- *A precise matrix of network discovery* on page 56
- *A tree of IPv4 ranges* on page 56
- *Property Groups* on page 59
- *Network Property Groups* on page 60
- *How to use Network Property Groups* on page 62
- *Create or modify a Network Property Group* on page 63
- *Apply a Network Property Group to a range* on page 65
- *Community Property Groups* on page 65
- *More on community strings* on page 66
- *Property sets are a shortcut* on page 69

A precise matrix of network discovery

In chapter 5, *Set up Network Discovery* on page 49, there were instructions to set up discovery quickly and simply just to get started. The instructions were to apply the Network Property Group, “Active discovery”, to all of your IPv4 range or ranges and assign them one community string, “public”.

You can leave discovery set up that way, if it is satisfactory to you. In fact, if there is a lot of change in your network, leaving it alone may be the best thing to do. However, you *can* set discovery up more precisely. For instance, you may want to reduce overhead on the network, or you may have a lot of community strings for security reasons and want to set up separate ranges for them. You can pick out IPv4 ranges or individual devices for Network Discovery to handle differently.

Network Discovery allows you to set up a matrix of network discovery, analyzing your network both geographically and functionally. For example, you might arrange discovery for an IPv4 range in a particular building one way and single out all the routers or servers across your network another way.

A tree of IPv4 ranges

Network Discovery actually works harder when it doesn't find devices than when it does, because it keeps trying. Once Network Discovery has been running for a while, you may know that some ranges can be deleted or that they need less than full active discovery.

On the other hand, you may decide you want even more information from certain ranges. Perhaps you want to turn on resource management to have disk and CPU information from servers or printers

So far, you have Network Discovery set up to examine every device the same way. If you want to look at some parts of the network or some individual devices differently or not at all, add ranges that you want to have treated differently. You can then apply Property Groups to the ranges.

You will be creating a tree of ranges and the tree can be as complicated as necessary to have Network Discovery monitor your network the way you want.

Note: A range can consist of one device. The starting and ending IPv4 addresses are the same.

Note: If you decide that two adjacent IPv4 ranges really should not be separate, you can merge them. The ranges must have identical properties or you cannot merge them.

To merge IPv4 ranges

1 Administration > Network configuration > Merge IPv4 ranges

Network Discovery displays all adjacent ranges sharing identical properties along with what the results of merge will be.

2 Enter the two ranges you want to merge.

3 Click **Merge**.

You have merged two IPv4 ranges in your proposed new configuration, but your change will not take effect until you activate your change.

Figure 6-15: Example of a developed network tree as shown in “List IPv4 ranges”

IPv4 Range	Property Set/Group Name
--[0.0.0.0 to 255.255.255.255]	Set: global
--[10.56.5.254 to 10.56.5.254]	Network: Active discovery
--[172.22.1.1 to 172.22.7.255]	Network: Active discovery
--[172.22.1.1 to 172.22.3.255]	Network: Resource manage
--[172.22.1.1 to 172.22.1.1]	Network: Unmanaged router
--[172.22.4.0 to 172.22.4.255]	Network: Do not allow discovery
--[172.22.4.0 to 172.22.4.255]	Network: Do not resource manage
--[172.22.5.240 to 172.22.5.255]	Network: Do not allow discovery
--[172.22.5.240 to 172.22.5.255]	Network: Do not resource manage
--[172.22.10.0 to 172.22.10.255]	Network: Active discovery
--[172.22.11.0 to 172.22.11.255]	Network: Active discovery
--[209.167.240.0 to 209.167.240.127]	Community: default 0
--[209.167.240.0 to 209.167.240.127]	Network: Active discovery
--[209.167.240.1 to 209.167.240.127]	Network: Resource manage
--[209.167.240.2 to 209.167.240.2]	Network: DHCP server
--[209.167.240.3 to 209.167.240.3]	Network: DHCP server
--[209.167.240.7 to 209.167.240.7]	Network: DHCP server

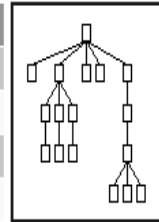
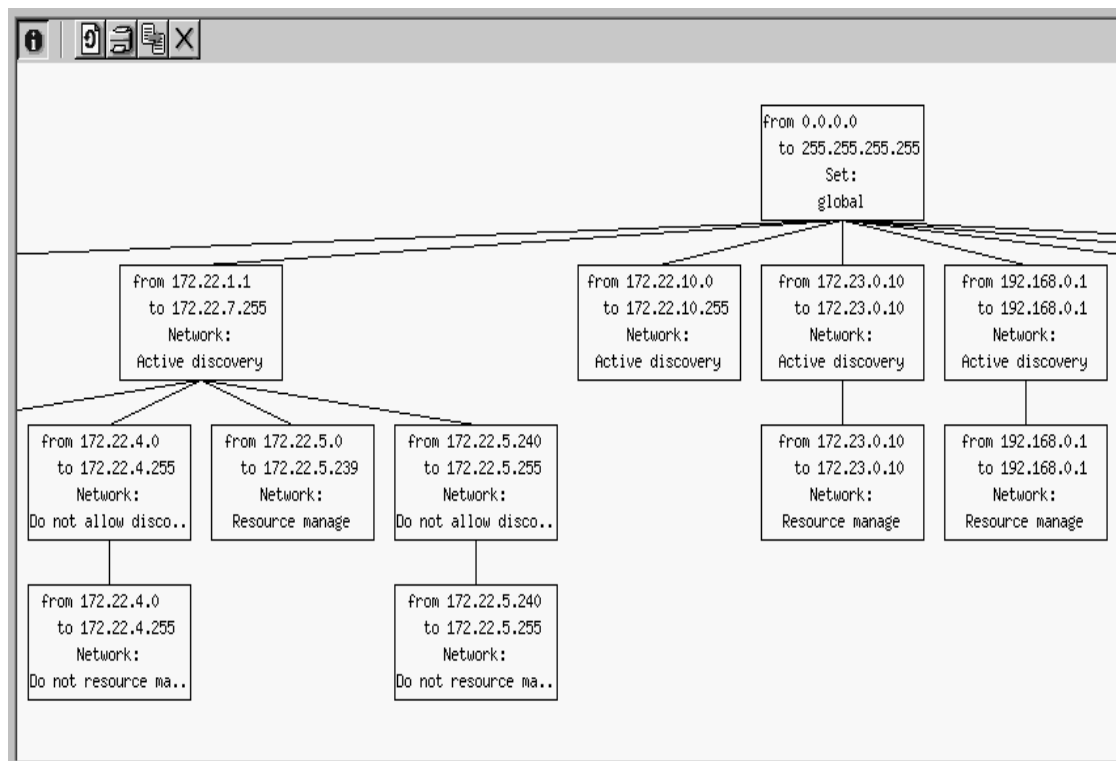


Figure 6-16: Part of a developed network tree as shown in “Review changes”



Property Groups

Network Discovery comes with default property groups you can apply to the IPv4 ranges you set up. A property group contains characteristics or properties that distinguish a range from other ranges, especially from its parent range. You can also modify the default Property Groups and create new ones.

There are two kinds of property groups:

- Network—for properties that govern network discovery
- Community—for community strings

Network Property Groups

It is unlikely you will want to modify the default Network Property Groups or create new ones. The defaults will probably be sufficient.

To see a list of all Network Property Groups

- ▶ **Administration > Network configuration > Network Property Groups > List Network Property Groups**

The list is a table with the names of the groups on the left and the names of the properties across the top.

Figure 6-17: List of default Network Property Groups

Name	IPv4 Ranges	Allow devices	Actively ping	NetBIOS query	Resource manage	Force ARP table read	Accumulate IP Addresses	Allow IP Addresses	Allow ICMP and SNMP	Device Modeler Interval
<u>global</u>		off	off	off	off	off	off	on	off	4 days 0 hours
	Site-wide defaults									
<u>Active discovery</u>		on	on	on	off	off	off	on	on	inherit
	Actively ping network and allow devices to be discovered									
<u>Do not allow discovery</u>		off	off	off	off	off	off	on	off	inherit
	Do not allow this network range to be discovered									
<u>Resource manage</u>		on	on	on	on	off	off	on	on	inherit
	Discover network and apply resource management									
<u>Do not resource manage</u>		on	on	on	off	off	off	on	on	inherit
	Do not apply resource management									
<u>Unmanaged router</u>		inherit	inherit	inherit	inherit	inherit	on	inherit	inherit	inherit
	Allow IP addresses to accumulate, useful for unmanaged routers									
<u>DHCP server</u>		inherit	inherit	inherit	inherit	on	inherit	inherit	inherit	inherit
	Forces ARP table to be read, useful for DHCP servers									
<u>Restrict to scanned-only</u>		on	off	off	off	off	off	on	off	inherit
	Restrict this range to scanned-only devices									
<u>All off</u>		off	off	off	off	off	off	off	off	inherit
	Do nothing for this range									

<u>Passive discovery</u>	on	off	inherit	inherit	off	off	on	on	inherit	
	Passively discover network, no ping sweep									
<u>NAT</u>	off	off	off	off	off	off	off	off	inherit	
	Range used for network address translation, do not allow discovery or add to device model									
<u>Service manage</u>	on	on	on	inherit	off	off	on	on	inherit	
	Discover network and apply service management									
<u>Do not service</u>	on	on	on	inherit	off	off	on	on	inherit	

The properties

Each Network Property Group contains the same properties, but the value of each property is different—“on,” “off,” or “inherit”—depending on the group. If a group “inherits” a value, it takes whatever value belongs to the parent range of any range the group is applied to. The following properties are in every Network Property Group:

- **Allow devices**—Allow devices to be added
- **Actively ping**—Actively ping devices for discovery
- **NetBIOS query**—Query devices for their NetBIOS names (the computer user names)
- **Resource Manage**—Query devices for resource management
- **Force ARP table read**—Force ARP table to be read
- **Accumulate IP Addresses**—Accumulate IP Addresses instead of replacing them
- **Allow IP addresses**
- **Allow ICMP and SNMP**
- **Device modeler interval**

Note: The device modeler interval is not “on,” “off,” or “inherit”, but rather “set” or “inherit”. If the value is set, it is set to a specific time.

How to use Network Property Groups

Some of the property groups cause Network Discovery to give you more data than others, but in doing so they also generate more traffic on the network. It can be a trade-off, a balance between efficiency and performance. You might choose to do less discovery on some parts of the network and more on others.

Table 6-4: Default Network Property Groups that increase functionality (and traffic)

Property Group	Purpose
global	The starting point, assigned to the 0–255 range. Almost completely set to off.
Active discovery	Ping, poll, table read. Find devices and information about them to add to database.
Resource manage	The most active of the Network Property Groups. In addition to Active discovery, provides disk, CPU, and memory information from servers, printers or UPSes.
Unmanaged router	In this Property Group, Accumulate IP addresses is set to “on”. For routers that do not have SNMP management enabled.
DHCP Server	This Property Group has ARP table read set to “on”. For servers providing Dynamic Host Configuration Protocol (DHCP) services, or for any other device (except routers) with a large ARP cache.

Table 6-5: Default Network Property Groups that decrease functionality (and traffic)

Property Group	Purpose
Do not allow discovery	For ranges that you do not want Network Discovery to ping and poll.
Do not resource manage	Do not resource manage has the same property values as Active Discovery . Use it as a “child” range of a Resource Manage range.
Passive Discovery	Network Discovery does not actively look for devices, but will include them if it happens to find them. (For example, Network Discovery may be able to gather the information from the ARP cache of a device.)
Restrict to scanned only	For IPv4 ranges where there are only devices that should be found by Express Inventory (the WMI collector).
NAT	Network Address Translation (NAT) allows a device model to appear, but blocks its IP address. Useful for removing duplicate or incorrect IP addresses.
All off	The least active of the default Property Groups. All values are set to off. For use when it’s easier to turn a range off than to delete it.

Create or modify a Network Property Group

You are unlikely to need to know how to create, modify, or delete Network Property Groups. The default Network Property Groups will almost certainly meet your needs, but if they don’t, here are the instructions.

Note: If a Property Group has been altered, the shortcut menu of “add”, “modify”, and “delete” has an additional entry, “Reset to default”.

Modify a Network Property Group

Modify a Network Property Group

- 1 **Administration > Network configuration > Network property groups > Modify a network property group**
- 2 Select the Network Property Group you want to modify.
- 3 For each parameter, click **On** or **Off** or **Inherit**.
- 4 Click **Submit Property Group**.

Note: Before you can delete a Property Group, you must remove it from any IPv4 ranges to which it has been applied. If the Property Group belongs to a Property Set that has been applied to a range, you can delete the Property Group. The Property Set will then set the deleted value to “inherit”.

Create a Network Property Group

Add a Network Property Group

- 1 **Administration > Network configuration > Network Property Groups > Add a Network Property Group**
- 2 Give your new Property Group a name.
- 3 Give your new Property Group a description.
- 4 For each parameter, click **On** or **Off** or leave it at the default value, **Inherit**.
- 5 Click **Submit Property Group**.

Delete a Network Property Group

You can delete a Network Property Group that no longer meets your needs and is just cluttering up the list.

Delete a Network Property Group

- 1 **Administration > Network configuration > Network Property Groups > Delete a Network Property Group**.
- 2 Select the Network Property Group you want to delete.
- 3 Click **Select**.
- 4 Click **Delete**.

Note: You cannot erase default Property Groups.

Apply a Network Property Group to a range

You might think of it as adding ranges that you want to *subtract* in some way from the preceding range. Each successive range that you add takes all its properties from the range of which it is a subset—except the properties you specify for it. The “child” inherits properties from its “parent,” except for the properties you give it.

For example, you might set up Network Discovery to resource manage all devices from 172.22.1.212 to 172.22.1.251 and then add (*subtract*) a range from 172.22.1.231 to 172.22.1.239 to which you will assign the Network Property Group, “Do not resource manage.”

The range we added in the previous example, 172.22.1.231 to 172.22.1.239, inherits whatever device modeler interval belongs to its parent range, 172.22.1.212 to 172.22.1.251.

In other words, the “child” range with the Network Property Group, “Do not resource manage,” inherits the “device modeler interval” value of the “parent” range that has the Network Property Group, “Resource manage.”

Community Property Groups

Community Property Groups allow you to create lists of community strings to apply to different portions of your network. The one default Community Property Group is “global.” If you are not sure what strings apply to your devices or subnets, you can add all of your community strings to this global list.

If you are more concerned with security, and you have community strings for particular devices or subnets, you can create a Community Property Group with a “list” of strings. You then apply the Community Property Group to the IPv4 range or ranges. Remember that you must activate any changes to the system in order to have the changes take effect.

To create a Community Property Group

- 1 Administration > Network configuration > Community Property Group > Add a Community Property Group
- 2 Give a name to the Community Property Group. Use a name that is meaningful to you.

- 3 Add a description.
- 4 Under the heading **Add a Community String** enter a string name, and select the appropriate **Type** (**read** or **write**, or both).
When you add community strings, the order is important, enter the most frequently used strings first.
- 5 Click **Add**.
- 6 Repeat steps 4 and 5 for each community string that can be applied to the same set of devices or subnets.
- 7 If necessary, select a community string and click the **Move Up** or **Move Down** buttons to move it to the right place.
- 8 Click **Submit**.

To apply the Community Property Group to the IPv4 range

- 1 Click **Administration > Network configuration > Add IPv4 range**.
- 2 Click **Add by interval** and enter the starting and ending IPv4 addresses for the range you want.
- 3 In the **Choose existing Property Set/Group** drop-down list, select the name of your newly created Community Property Group.
- 4 Click **Submit**.

More on community strings

If you do not add any community strings, but keep “public” (the default) in the list, Network Discovery will attempt to read the MIB of all devices in the defined IP range or set of ranges using only “public.” Network Discovery will not be able to write to the MIBs of any devices, since it has been given no write community strings.

Note: If you do not add any community strings and delete “public” from the global Community Property Group (that is, if no community strings are defined,) Network Discovery will not interrogate any devices in your network. As a result, Network Discovery will discover devices but may not be able to identify them.

Warning: Do not delete “public” from the global Community Property Group unless you are absolutely sure you do not need it.

Multiple Strings

For each device that it discovers, Network Discovery will try all the community strings you have provided for that device and use the first string that receives a positive acknowledgement to read or write the MIB. This means that Network Discovery may try several community strings before it finds one that will cause the device to respond.

The fact that Network Discovery may try several community strings has implications for any devices that issue SNMP traps (also known as security traps and authentication traps).

SNMP Traps

Some devices may issue an SNMP trap when Network Discovery attempts to explore them. Even if Network Discovery has the correct community string in its list, Network Discovery may still “trip” the trap if Network Discovery tries multiple community strings before finding the right one.

For example, Network Discovery might try two invalid community strings before reaching the valid community string. Any invalid community string will “trip” a security trap.

Once a trap has been tripped, the trap may be re-issued periodically until the trap is reset. Network Discovery does not reset traps. Therefore, you should either disable all such traps or use only a single correct community string for each device that issues a trap.

Note: If another network management system is used in the same network with Network Discovery, this other system may generate alarms due to these traps.

Directed Community Strings

If a device is programmed with a directed community string (sometimes known as a direct access list), it will reject the attempt by Network Discovery to explore it, even if Network Discovery has been given the correct community string. With a directed community string, each device checks not only the “password,” but also to see if the Peregrine appliance is on the list of “trusted” devices.

You can allow Network Discovery to communicate with a device with a directed community string, but you cannot do so merely by configuring Network Discovery. You must also give the device itself an entry for a directed community string associated with the IP address of the Peregrine appliance.

Deleting a community string

You can delete a single community string, or you can delete an entire Community Property Group of community strings. Be sure you know which procedure you want to perform.

You cannot delete an entire Community Property Group if an IP v4 range is using it.

To delete a single community string

- 1 Click **Administration > Network Configuration > Community Property Groups > Modify a Community Property Group**.
- 2 Select a Community Property Group from the pull-down list.
- 3 Click **Select**.
- 4 Under the “Delete a Community String” heading, select the community string you want to delete and click **Submit**.

You have deleted a single community string from a Community Property Group in your proposed configuration, but your change will not take place until you activate changes.

To delete a Community Property Group

- 1 Click **Administration > Network configuration > Community Property Groups > Delete a Community Property Group**.
- 2 Select a Community Property Group from the pull-down list and click **Select**.
- 3 Click **Delete**.

You have deleted a Community Property Group from your proposed configuration, but your change will not take place until you activate changes.

Property sets are a shortcut

The use of Property Sets is optional. A Property Set is a collection of Property Groups. Applying a Property Set to a range is a convenient way of applying more than one Property Group at a time.

For example: If you find you are setting up several ranges and applying the Network Property Group, “Active discovery”, and then setting up the same ranges with a Community Property Group you have defined, you might find it easier to create a Property Set, Property Set “X” that contains the Network Property Group, “Active discovery” and your Community Property Group with the strings you added. It’s a shortcut to save you from entering IPv4 ranges more than once.

You can list, add, modify and delete Property Sets, the same way you do with Property Groups.

Figure 6-18: Default Property Sets

Name	IPv4 Ranges	Network Property Group	Community Property Group	Scanner Property Group	Listener Property Group
<u>Set: global</u>	0.0.0.0 to 255.255.255.255 (4,294,967,296 devices) Site-wide defaults	<u>Network: global</u>	<u>Community: global</u>	<u>Scanner: global</u>	<u>Listener: global</u>
<u>Set: All off</u>		<u>Network: All off</u>	<u>Community: All off</u>	<u>Scanner: All off</u>	<u>Listener: All off</u>
<u>off</u>	Do nothing for this range				

Reviewing and activating your configuration changes

Remember that you must activate any changes to the system in order to have the changes take effect. You can go straight to activating the change as we did in chapter 5. If you have made a lot of changes, you should first review the setup and the changes.

To review proposed changes

- 1 Click **Administration > Network configuration > Review changes**

A tree diagram of your proposed IPv4 ranges appears, along with a table detailing all the changes made in this section.

Network Discovery tells you how many potential devices it will have to explore, and how long it will take (for example, “at least 33 minutes”).

You will shown any configuration problems detected by Network Discovery. You can ignore the warnings, but do so at your own risk.

- 2 If you wish to see details on the proposed changes to the IPv4 ranges, you can click on the tree diagram to expand it.

New ranges appear in green. Changes to existing ranges are in yellow.

- 3 Review the changes to make sure the new configuration is correct. If you decide to implement the changes you have made, applying the changes will update your network configuration. You can also discard all changes.

To discard current changes

- 1 Click **Administration > Network configuration > Review**.
- 2 Click **Undo**.

7 Accounts

CHAPTER

Once you have set up the Peregrine appliance and configured Network Discovery, you will want to set up accounts. For each account, you can set the name, password, and other important information. Make sure anyone who needs to work with Network Discovery has an account, and knows the limits of their account level.

Topics in this chapter include:

- *There are four pre-installed accounts on page 72.*
- *How many people can use Network Discovery at once on page 72.*
- *How the types of accounts differ on page 72.*
- *Creating accounts on page 74.*

There are four pre-installed accounts

Network Discovery comes with four accounts pre-installed, one of each type:

- Demo
- IT Employee
- IT Manager
- Administrator

The Network Discovery Administrator must create any other accounts.

Figure 7-19: List of pre-installed accounts

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

How many people can use Network Discovery at once

Network Discovery supports a maximum of 250 accounts.

More than one account can be used at a time. Up to six accounts can view a Network Map simultaneously. Up to 20 accounts can use any part of Network Discovery other than the Network Map simultaneously.

How the types of accounts differ

Each type of account has different permissions. The principal difference between the types of account is the amount of administration permitted.

- Demo—limited control, “safe” for demonstration and training
- IT Employee—can make some changes that affect what their own account sees
- IT Manager—can make changes that affect what other accounts see
- Administrator—the most powerful, sets up network discovery, sets up more accounts

Warning: While it is possible to create more than one Administrator account, we recommend you have only one Administrator account. That account should be reserved for use by the Network Discovery Administrator. If you have more than one Administrator account, there is a danger that each Administrator account will overwrite the work of all others.

Table 7-6: What the accounts can do

	Demo	IT Employee	IT Manager	Administrator
Network Map				
Initial map configuration file	Copy of Prime	Copy of Prime	Copy of Prime	Copy of Prime
Default map configuration file	Copy of Prime	last saved or used	last saved or used	last saved or used
Open any saved map configuration	YES	YES	YES	YES
Save any number of map configurations	YES	YES	YES	YES
Save a map configuration as Prime	—	—	YES	YES
Change a device icon	—	—	YES	YES
Change a package icon	YES	YES	YES	YES
Change a device's priority	YES	YES	YES	YES
Change a device's notification priority	—	—	YES	YES
Alarm Thresholds	view	view	view + change	view + change
Purge a device	—	—	YES	YES
Reset MTTR and MTBF for a device	—	—	YES	YES
Disconnect other accounts' map sessions	—	—	—	YES
Managers (for example, Device Manager)				
View read and write community strings for device	—	—	YES	YES
View and use <i>set</i> link to MIB Browser	—	—	YES	YES
SNMP query default string	“public”	“public”	from Network Discovery	from Network Discovery

	Demo	IT Employee	IT Manager	Administrator
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
Disconnect other accounts' map sessions	—	—	—	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

Creating accounts

To create a usable account, you must add an account, then assign a password.

You can also modify the properties of the account and the contact data for the person who owns the account. This is optional; the account owner can perform these actions on his or her own account.

Whether you just create an account or whether you customize each account for each owner is your decision. You may consider such factors as the number of accounts to be created, how knowledgeable each account owner is, and the restrictions of your work environment.

To create an account

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

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

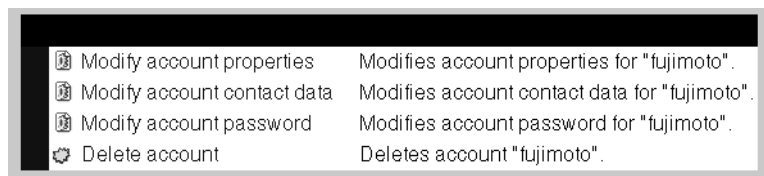
- a through z
- 0 through 9
- underscore (_) (the underscore cannot be the first character in the account name)

- 3 Click **Add Account**.
 - You have created an IT Employee account.

Note: Even though the account has been created, it cannot be used until you assign it a password. An account without a password is considered disabled. The account owner will not be able to use it to log in to Network Discovery.

After you create an account, a shortcut menu appears.

Figure 7-20: Brief menu for adding an account



You can use the shortcut menus to continue working with the account.

To create a password for an account

Note: Alternative: If you see a brief menu on the screen, click **Modify account password**, then skip to step 4.

- 1 Click **Administration > Account administration > Account password**.
- 2 Select the account from the list box.
- 3 Click **Modify Account**.
- 4 Enter an account password in both boxes.

Figure 7-21: Entering an account password

- 5 Click **Modify Password**.
- The account may now be used.

You can change the account type or customize any of its other properties in **Administration > Account administration > Account properties**. For more detail, see the *Network Discovery User Guide*.

To change an account type

Note: Alternative: If you see a brief menu on the screen, click **Modify account properties**, then skip to step 4.

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

Note: You should have a single Administrator account. That account should be reserved for use by the Network Discovery Administrator. If you have more than one Administrator account, there is a danger that each Administrator account will overwrite the work of all the others.
- 5 (optional) Change any other account properties, as appropriate.

For example, you may prefer to enter the full name of the account owner.
- 6 Click **Modify Properties**.

8 Backup and Restore

CHAPTER

Every day, after midnight, Network Discovery saves its data to a backup partition on the Peregrine appliance. In addition, you have the option of saving the data externally to an FTP site or to a tape. If necessary, you can restore the data from either the internal or the external backup or, if necessary, from another Peregrine appliance.

Topics in this chapter include:

- *About external backups on page 78*
- *Choosing tape or an FTP site for your external backup on page 79*
- *Configuring an external backup on page 79*
- *Testing your external backup and restore on page 81*
- *To run an internal or external backup immediately on page 82*
- *Restoring your data on page 82*

About external backups

Because the Peregrine appliance has room for only one backup, you may choose to back up your data to an FTP server or (for the smaller version of the Peregrine appliance) to a local USB tape drive. If you choose either of these methods (or both), you will be able to save a backup of your network data every day.

If you decide to store external backups, Network Discovery performs two separate functions. Every day, after midnight, Network Discovery creates an internal backup. Once the internal backup is complete, Network Discovery sends that internal backup to the FTP site and/or to the USB tape drive.

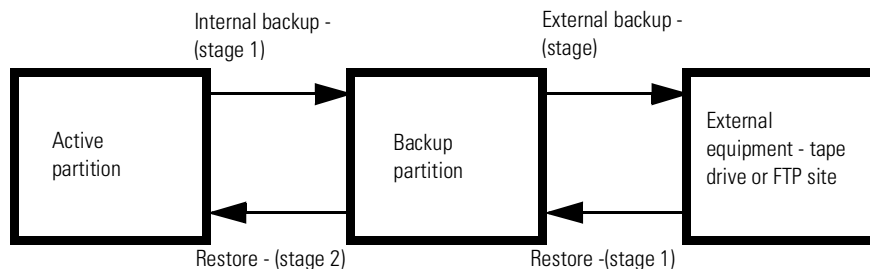
When you restore data, you also have two options. You can restore either from the internal backup or from the external backup.

Important: When you successfully restore from a backup, Network Discovery assumes that all events are in an OK status for the first sampling period.

There may be phantom alarms and warnings on the Health Panel for the first sampling period, because the events log has been affected by restoring from an old backup.

Note: You cannot back up directly from the active partition to the external backup, and you cannot restore from the external backup directly to the active partition.

Figure 8-22: A conceptual diagram of Backup and Restore showing all stages



Choosing tape or an FTP site for your external backup

Data can be backed up to:

- a USB tape drive
- a file on any device that supports the File Transfer Protocol (FTP)

The following FTP servers have been tested for use with Network Discovery:

- Windows 95, Windows 98, Windows 2000, and Windows NT running IIS
- Red Hat Linux: Kernel 2.2.12, FTP version FTP-wu.2.5.0(1)

For a recommended USB tape drive, see *Appendix B, Extra Hardware* on page 95.

Note: For FTP backups, you must have read/write permission on the repository device.

Tip: For increased security on FTP backups, create a special account on the repository device with very few security privileges.

If you do not have a device that supports FTP nor a user name and password for that device, ensure that the FTP option is Off. The default is Off.

Data is backed up to the external device every 24 hours, beginning after midnight when *any* option is on.

Configuring an external backup

To configure an external backup

- 1 Click **Administration > Backup and Restore > External backup configuration**.
- 2 Click **FTP On** or **Off**.
- 3 Click **Tape On** or **Off**.

If you do not have a USB tape drive connected to your Peregrine appliance, ensure that the tape option is Off.

The default is Off.

Note: The tape option does not appear if you do not have a tape drive connected. However, the tape option *does* still appear, if you disconnect the tape drive after you have configured the external backup as “Tape On”.

Note: If you have just restored a backup from an older appliance that did have a tape drive installed, the tape option may appear even though you no longer have a tape drive installed.

To back up your network data to an FTP site

- 1 Click **Administration > Backup and restore > External backup configuration**.
- 2 In the FTP section of the page, activate the On button.
- 3 Enter the user name (required).
 - *valid characters:* A–Z, a–z, 0–9 @ (at symbol), . (period), - (hyphen)
 - *length of input:* 4–50 characters
- 4 Enter the password for the FTP server (required).
 - *length of input:* 4–20 characters
- 5 Enter the host name or IPv4 address of the FTP server (required).
 - *valid characters:* A–Z, a–z, 0–9 @ (at symbol), . (period), - (hyphen)
 - *valid length of input:* 1–50 characters
- 6 If necessary, enter the directory to which the backup file should be saved.
 - *valid characters:* any
 - *length of input:* 0–256 characters
- 7 If necessary, enter the name of the backup file.
 - *valid characters:* any, except / (slash) and \ (backslash)
 - *length of input:* 1–256 characters

The default file name will be the current date in an 8-digit format: YYYYMMDD. If you want another date format, you can use the Help available to select a preferred format. For example, if you enter the filename “backup_%d_%B.tar” you will get filenames with a numeric day of the month (ex. 20) and a month (ex. May).

Note: Make sure you pick a format that is compatible with the operating system running on your FTP server. Some operating systems will not interpret slashes (/) or colons (:) as valid characters.

- 8 Enter the port number of the FTP site to which you are connecting.
 - 1–65, 535

- 9 If Network Discovery has been set up for e-mail, choose whether or not Network Discovery will send e-mail on success and on failure and to whose e-mail address.
- 10 Choose whether or not you will back up scan files.
- 11 Click **Submit**.
Network Discovery will now back up its data to the FTP site once a day.
- 12 You can check the backup log at any time by clicking **Administration > Backup and restore > View backup log**.

The list of backups is sorted by time and date.

Testing your external backup and restore

To make sure you have entered the correct information for your FTP server, you can test the link. You can also test the external backup to tape (if a tape drive is configured).

To test your external FTP backup

- 1 Click **Administration > Backup and restore > Test external backup**.
- 2 Select **FTP**.
- 3 Click **Test**.

A screen appears showing your FTP configuration information.

- 4 Click **Confirm**.

A message appears, telling you if the test was successful or not.

To test your external tape backup

Important: Testing (running) an external tape backup erases any data previously stored on the tape.

- 1 Click **Administration > Backup and restore > Test external backup and restore**.
- 2 Select **tape**.

A message appears, telling you if the test was successful or not.

To run an internal or external backup immediately

Creating an external backup

If you select this option, you will send the existing internal backup (which was created after midnight) to tape or FTP right now.

To back up your data immediately

- 1 Click **Administration > Backup and restore > Run external backup now**.
- 2 Click **Backup now**.

Creating an internal backup

If you select this option, you will send the active data to the backup partition immediately.

Note: If Network Discovery is configured to run an external backup, forcing an internal backup forces an external backup too.

Note: Forcing a backup does not prevent the automatic daily backup from happening.

To back up your data immediately

- 1 Click **Administration > Backup and restore > Run internal backup now**.
- 2 Click **Backup now**.

Restoring your data

You can restore your network data from the internal backup. If you have configured external backups, you can restore your data from a USB tape or from an FTP site. You can also restore data from another Peregrine appliance, for instance, if you are upgrading from IND 4.2 or 4.3.

Note: To restore your data to the active partition, Network Discovery must restart its software; Network Discovery functions will not be available.

Restoring from the internal backup

Network Discovery creates an internal backup every night. You can restore your data from this backup if you need to do so.

To restore your data from an internal backup

- 1 Click **Administration > Backup and restore > Restore from internal backup**.
- 2 You can choose whether or not you will keep your current scan files if there are none in the backup.
- 3 If Network Discovery has been set up for e-mail, choose whether or not an e-mail notification will be sent and to whose account.
- 4 Click **Restore**.
- 5 You can check the restore log by clicking **Administration > Backup and restore > View restore log**.

Restoring from an FTP site

If you have configured Network Discovery to back up an FTP site, you can use this procedure to restore your data.

To restore your data from an FTP site

- 1 Click **Administration > Backup and restore > Restore from FTP**.
- 2 You can choose whether or not you will keep your current scan files if there are none in the backup.
- 3 If Network Discovery has been set up for e-mail, choose whether or not an e-mail notification will be sent and to whose account.
- 4 Click **Restore**.
- 5 When the backup is complete, you can check the restore log by clicking **Administration > Backup and restore > View restore log**.

Restoring from tape

If you have configured a backup USB tape drive, you can use this procedure to restore your data.

To restore your data from a tape

- 1 Click **Administration > Backup and restore > Restore from tape**.
- 2 You can choose whether or not you will keep your current scan files if there are none in the backup.
- 3 If Network Discovery has been set up for e-mail, choose whether or not an e-mail notification will be sent and to whose account.
- 4 Click **Restore**.

- 5 When the backup is complete, you can check the restore log by clicking **Administration > Backup and restore > View restore log**.

Restoring from another appliance

Use a cross over cable to connect the two appliances. This procedure is useful for migrating data from one appliance to another in order to upgrade from IND 4.2 or 4.3 or from Xanadu 1.0.4.

To restore your data from another appliance

- 1 On the new appliance, click **Administration > Backup and restore > Restore from another appliance**.
- 2 If Network Discovery has been set up for e-mail, choose whether or not an e-mail notification will be sent and to whose account.
- 3 Click **Restore**.
- 4 When the backup is complete, you can check the restore log by clicking **Administration > Backup and restore > View restore log**.

9 To Upgrade from InfraTools Network Discovery

CHAPTER

The hardware of the Peregrine appliance is different from the InfraTools appliance but you can migrate your data to upgrade your IND appliance by following the procedures in this chapter.

You can upgrade to PND from any of the following Peregrine IND software packages:

InfraTools Network Discovery	4.2.0, 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.5 4.3.0 or 4.3.1
Xanadu	1.0.4

Topics in this chapter include:

- *How it works* on page 86
- *Configure your corporate firewall* on page 86
- *Upgrade the license on your new appliance* on page 87
- *Ensure that you have a backup from your old appliance* on page 87
- *Restore the old data to the new appliance* on page 87
- *You can keep your IND Seeds, Blocks and Forces* on page 88

How it works

Essentially, the process is to take a backup from your old appliance and restore it on the new one. To upgrade your InfraTools Network Discovery or Xanadu appliance, perform the following tasks in the following order.

Table 9-7: What to do when you upgrade from IND

Task	Where to get information
Get started and prepare	Chapter 1, <i>Welcome to Network Discovery</i> on page 5
Install the new appliance and start Network Discovery	Chapter 2, <i>Install and Start Network Discovery</i> on page 15
Log in to your new appliance	Chapter 3, <i>Appliance Management</i> , up to and including <i>Log in to Network Discovery</i> on page 24
Request and install your license on the new appliance	Chapter 4, <i>Licenses</i> on page 45
Take the backup from your old appliance and install it on the new one.	This chapter, <i>To Upgrade from InfraTools Network Discovery</i> and the previous chapter, Chapter 8, <i>Backup and Restore</i> on page 77.
Complete appliance management	Return to Chapter 3, <i>Appliance Management</i> , and carry on from and including <i>How to shut down the Peregrine appliance</i> on page 27 and so on...

Configure your corporate firewall

Access to Peregrine Systems Customer Support has been simplified and made more secure by means of SecureShell (SSH). You now need to provide access on fewer ports and can close some ports that you had open for IND.

For customer support by way of the Internet, configure the corporate firewall to allow the Peregrine Systems IP address 209.167.240.9 (sprocket.loran.com) to make inbound connections on the following ports:

- 22/tcp (SSH)
- 80/tcp
- 8100/tcp through 8105/tcp
- 8108/tcp

To preserve the integrity of your firewall, close the following ports. They are no longer necessary.

- 2120 (FTP)
- 2121 (FTP)
- 2323 (Telnet)

Upgrade the license on your new appliance

Licenses from InfraTools Network Discovery or Xanadu 1.0 are not compatible. You must upgrade to the Peregrine Network Discovery license.

The Peregrine appliance comes to you with a default license installed, but you will want to upgrade the appliance to all you are entitled to.

- 1 Log in, following the instructions in *Log in to Network Discovery* on page 24.
- 2 Follow the instructions in Chapter 4, *Licenses* on page 45.

Ensure that you have a backup from your old appliance

- ▶ Following the procedures in *Backup and Restore* on page 77, make sure that you have the backup you want to use.

Note: The backup must be from an internal backup, an FTP server, or a tape drive. (The tape drive for the old appliance must have a SCSI connector.)

Note: It's simpler to skip the external backup step and use the internal backup, but you may feel safer having the external backup as well.

Note: The upgrade procedure uses the last backup, not what is currently running. You may wish to run an internal backup now to have up-to-the-minute data.

Restore the old data to the new appliance

- 3 Connect the cross over cable that came with the IND appliance to the new Peregrine appliance.

On the IND appliance, connect to the cross over connection.

On the IBM xSeries server version of the Peregrine appliance, connect to ethernet port 2 on the bottom left.

- 4 Following the procedures in *Backup and Restore* on page 77, restore the backup you want to use.

Your software and licenses have been upgraded. You can now use PND. Continue with the procedures in Chapter 3 *Appliance Management* on page 23.

You can keep your IND Seeds, Blocks and Forces

If you have upgraded from InfraTools Network Discovery 4.2. or 4.3, you will still be able to use the “old style” interface that you had set up with Seeds, Blocks, and Forces. However, once you activate any changes to the Network configuration pages, the old interface will be removed. If you ever need to make changes to your IND configuration go to **Administration > IND 4 style network configuration**. For more information, refer to your IND documentation.

10 Before you call...

CHAPTER

You can save yourself some time, if you make sure your Peregrine appliance has the most up-to-date software before you contact Peregrine Systems Customer Support.

Topics in this chapter include:

- *Overview on page 90*
- *Check that your maintenance license is current on page 90*
- *Check that you have the latest software components on page 90*
- *Download the new components to your appliance on page 90*
- *Install the new component(s) on page 91*
- *After you install new components on page 91*

Overview

Your problem could be something like, “Why doesn’t Network Discovery show me the router we just bought?” Your problem may be solved in the latest software.

It is difficult for Peregrine Systems Customer Support to investigate issues in older releases and quite frequently an issue is fixed in the latest release.

Check that your maintenance license is current

To check that you are still entitled to support

- 1 Click **Status > Network configuration > Current Settings > Installed Licenses**
- 2 See the value of the attribute, “Maintenance valid until.”

Check that you have the latest software components

To check that you have the latest software components

- 1 Click **Status > Network configuration > Current settings > Installed components**
- 2 In particular, see the value of the attributes, “jay” and “rulebase”.
Note: Peregrine Systems Customer Support may also ask you to ensure that other components are also active and installed. For instance, the hydra module and jay packages are tightly coupled and you may require a certain hydra version for a jay package to function and become active.
- 3 Compare your versions to the versions on the Peregrine Systems Customer Support web site. Check CenterPoint under “Network Discovery Downloads and Libraries” and see if the versions currently posted are newer than the versions currently installed on your Peregrine appliance.

Note: To access support.peregrine.com you must have an account.

Download the new components to your appliance

If the packages posted on the web site are newer than those currently installed on your Peregrine Appliance, download the latest software component(s).

Install the new component(s)

Pick a time to perform the upgrade when users are unlikely to be accessing Network Discovery. The Peregrine appliance will be unavailable for up to 30 minutes during the upgrade.

To install the new components

- 1 From the Windows **Start** menus, click **Run**.
- 2 Type `\\IPv4\share\packages\incoming`
where **IPv4** is the address of your Peregrine appliance
- 3 If you are asked to supply a user name and password, use the user name and password you use to log in to Network Discovery.
- 4 Drag and drop the new software component file into the above directory.
Network Discovery finds the new file and verifies it. Network Discovery also ensures that the maintenance contract is still valid. Then it performs the upgrade automatically.

Note: If your maintenance license had expired or if the component is not appropriate for installation, Network Discovery does not perform the upgrade and deletes the component file from the shared directory.



After you install new components

To check that the latest software component is installed

- ▶ **Status > Installed components.**

Changes are not instantaneous. You will not see changes in your data until the Device Modeler has updated. You can check to see when the Device Modeler last updated. You can also update the model.


To check when the Device Modeler last updated

- 1 On the Toolbar, click the **Network Map** button. 
- 2 On the Network Map, double-click a device.
The Device Manager opens.
- 3 Click the **Diagnosis** button. 

The Diagnosis panel opens.

Check when the Device Modeler last updated.

To update model

- 1 On the Toolbar, click the **Network Map** button. 
- 2 On the Network Map, double-click the device you are concerned about.
The Device Manager opens.

- 3 Click the **Update model** button. 

The device will go to the top of the device modeler's queue.

Note: There may be a delay of as much as 1–2 hours before the device appears on the Network Map.

If you still have a problem after the latest software components have been installed, and the device model has been updated, contact Peregrine Systems Customer Support.

A Security Checklist

APPENDIX

Although your Peregrine appliance will operate even if you do not follow these procedures, we strongly recommend that you take the following steps to reduce risk.

- 1 Place your Peregrine appliance behind your institution/corporation's firewall.

The Peregrine appliance stores a lot of information about your network. You do not want this information to be publicly available.

- 2 Change the write community string of the Peregrine appliance.

This is a documented community string, known to:

- admin accounts at your site
- existing and prospective Network Discovery customers

Anyone who knows the default write community string will be able to change the SNMP MIB of your Peregrine appliance.

- 3 Eliminate known account names “admin”, “itmanager”, “itemployee”, and “demo.”

- Create a new admin account for the Network Discovery Administrator.
- (optional) Create a new demo for training users.
- Log into the new admin account.
- Delete the accounts named “admin”, “itmanager”, “itemployee”, and “demo.”

These are documented account names, known to:

- users at your site
- existing and prospective Network Discovery customers

Anyone who knows the default account names may be able to gain access to your Peregrine appliance more easily, even if you have changed the passwords for the accounts.

- 4 Go to the **Event filter configuration** menu and modify the “email-admin-line” and “email-admin-device” filters.

You must direct e-mail from “admin” to the new account for the Network Discovery Administrator.

If you don't want to delete the accounts, at least do the following:

- Change the password for the “admin” account.

This is a documented account password, known to:

- anyone at your site with access to the Network Discovery documentation
- existing and prospective Network Discovery customers

Anyone who knows the default password for the “admin” account may be able to gain top-level access to your Peregrine appliance.

B Extra Hardware

APPENDIX

The following hardware is not supplied with the Peregrine appliance but is either required to provide extra functionality or is recommended.

Note: To connect all three pieces of equipment—a UPS, backup equipment and pager hardware—attach a Universal Serial Bus (USB) hub.

Uninterruptible Power Supply (UPS) units

Used for:

Protection against electrical service interruptions and fluctuations.

Note: Use of a UPS is strongly recommended. By default, if Network Discovery does not detect a UPS, it will issue a constant warning about the health of the Peregrine appliance.

Requirements

Any Smart-UPS, Back-UPS, or Back-UPS Pro UPS with a minimum rating of 1000VA and a USB connector. The connector must be USB.

Acceptable UPS units

A qualified UPS must be purchased separately by the user. Network Discovery will support any American Power Conversion Corporation UPS with a minimum rating of 1000VA and a USB connector.

Note: The Smart-UPS 1000 USB is the smallest recommended UPS, but larger ones may be used.

Recommended UPS units for Africa, Asia, Europe, Australia, the Middle East, and the South Pacific

Customers in Africa, Asia, Europe, Australia, the Middle East, and the South Pacific require a 230 volt UPS. The following tables list the small and large UPS units available for this voltage.

Small	
Model	Code
Smart-UPS 1000VA USB	SUA 1000I

Large	
Model	Code
Smart-UPS XL 1000VA USB	SUA 1000XLI
Smart-UPS 1500VA USB	SUA 1500I

Recommended UPS units for North America

Customers in North America require a 120 or 208 volt UPS. The following tables list the small and large UPS units available for this voltage.

Small	
Model	Code
Smart-UPS 1000VA USB	SUA 1000

Large	
Model	Code
Smart-UPS XL 1000VA USB	SUA 1000
Smart-UPS 1500VA USB	SUA 1500

Tape Drive

Used for:

Data backup

Required:

External USB tape drive, providing at least 20 gigabytes of uncompressed storage. The connector must be USB. The tape drive must work with Linux USB storage drive.

Recommended:

Seagate TapeStor Travan 40 Portable USB 2.0 -ST6401U2-R

External Modem

Used for

Alphanumeric paging

Required:

Must conform to ITU Recommendations V.32, V.22 bis, V.22, V.23, V.25, V.21 (that is, be able to operate from 1200 up to 9600 bits/second) *or better* (that is, may also conform to additional ITU Recommendations V.90, V.34, V.42, V.42 bis, V.32 bis, V.8 and so on.)

Operate by means of a well documented AT command set (that is, command set documentation must be available for the modem)

Must conform to local regulatory requirements for connection to the telephone network (FCC, DOC, JATE and so on.)

Must work with Linux ACM/USB drivers.

The connector must be USB.

