

Peregrine

# Network Discovery Setup Guide

---

Copyright © 2003 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 need technical support for this product, or would like to request documentation for a product for which you are licensed, contact Peregrine Systems, Inc. Customer Support by e-mail at [support@peregrine.com](mailto:support@peregrine.com).

If you have comments or suggestions about this documentation, contact Peregrine Systems, Inc. Technical Publications by e-mail at [doc\\_comments@peregrine.com](mailto:doc_comments@peregrine.com).

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

Peregrine Systems, Inc.  
Worldwide Corporate Headquarters  
3611 Valley Centre Drive San Diego, CA 92130  
Tel 800.638.5231 or 858.481.5000  
Fax 858.481.1751  
[www.peregrine.com](http://www.peregrine.com)



# Table of Contents

---

<b>Section 1</b>	<b>Preparing for Installation. . . . .</b>	<b>7</b>
<b>Chapter 1</b>	<b>Welcome to Network Discovery . . . . .</b>	<b>9</b>
	About Network Discovery . . . . .	10
	Why it's important to prepare. . . . .	10
	Start by collecting information about your network . . . . .	11
<b>Chapter 2</b>	<b>Pre-setup Questionnaire . . . . .</b>	<b>13</b>
	Your contact information . . . . .	13
	Describe your network's node and subnet setup. . . . .	14
	Enter the Peregrine appliance network information . . . . .	14
	Peregrine Systems Customer Support access . . . . .	15
	List IPv4 ranges for Network Discovery to discover . . . . .	15
	List IPv4 ranges for Network Discovery to avoid . . . . .	16
	List the community strings of your network's devices . . . . .	16
	Enter TCP/IP configuration . . . . .	17
	What server will you use for the Peregrine appliance? . . . . .	18
	Send the questionnaire. . . . .	19
<b>Chapter 3</b>	<b>Prepare the network . . . . .</b>	<b>21</b>
	Turn on SNMP management in all routers and core switches . . . . .	22
	Set DHCP lease time. . . . .	22
	(Optional) Turn on SNMP management in other devices. . . . .	23
	About community strings . . . . .	23
	Give the Peregrine appliance IP address to all devices using directed community	

	strings . . . . .	23
	(Optional) Adjust bridge aging . . . . .	24
	Plan the device and port to which the Peregrine appliance will be attached . . . . .	24
	Choose how to receive Peregrine Systems Customer Support . . . . .	24
	Enable firewall ports . . . . .	26
	Check Cisco devices . . . . .	28
	Check Committed Information Rate (CIR) values . . . . .	28
	Check the server that will be the Peregrine appliance. . . . .	28
	Check the management workstation . . . . .	31
<b>Section II</b>	<b>Installation . . . . .</b>	<b>33</b>
<b>Chapter 4</b>	<b>Install and Start Network Discovery . . . . .</b>	<b>35</b>
	About installing the hardware. . . . .	36
	Connect a keyboard and monitor directly to the Peregrine appliance . . . . .	36
	Set the BIOS boot sequence. . . . .	37
	Install Network Discovery software from the CD . . . . .	38
	Give the Peregrine appliance its network information . . . . .	39
	Connect the server to the network. . . . .	43
	Connect a management workstation to the network . . . . .	44
	Connect an Uninterruptible Power Supply (UPS) . . . . .	45
	Connect data backup equipment and pager hardware . . . . .	45
	(Optional) Connect the Peregrine appliance to a telephone line . . . . .	46
	Connect the Peregrine appliance to AC power. . . . .	46
	Optional use of terminal emulation software . . . . .	46
<b>Chapter 5</b>	<b>Appliance Management . . . . .</b>	<b>49</b>
	Log in to Network Discovery . . . . .	50
	How to shut down the Peregrine appliance . . . . .	53
	The Home page . . . . .	53
	The Toolbar . . . . .	54
	Assign a system name, contact, and location . . . . .	57
	Change the Peregrine appliance community strings . . . . .	57
	Set the time zone . . . . .	58
	Enter the domain name server . . . . .	59

	Enter the host name . . . . .	61
	Enter the Workgroup name. . . . .	62
	Enter the Administrator e-mail address . . . . .	63
	Enter the SMTP server . . . . .	63
	Set the system time . . . . .	65
	Change the default Admin password . . . . .	68
	About disabling warnings . . . . .	69
<b>Chapter 6</b>	Licenses . . . . .	71
	How it works . . . . .	72
	Request a new license . . . . .	72
	Install the new license . . . . .	73
<b>Chapter 7</b>	Set up Network Discovery . . . . .	75
	How it works . . . . .	76
	Set up the IPv4 range(s) to discover . . . . .	76
	Set up the IPv4 range(s) to avoid . . . . .	78
	Add ranges for DHCP servers and unmanaged routers . . . . .	78
	Add community strings—the quick way . . . . .	79
	Activate your proposed changes . . . . .	80
	Check that it's working. . . . .	80
<b>Chapter 8</b>	Refining Network Discovery . . . . .	83
	A precise matrix of network discovery . . . . .	84
	A tree of IPv4 ranges. . . . .	84
	Property Groups . . . . .	86
	Network Property Groups . . . . .	86
	How to use Network Property Groups . . . . .	89
	Making changes to Network Property Groups. . . . .	90
	Apply a Network Property Group to a range . . . . .	92
	Community Property Groups. . . . .	92
	More on community strings . . . . .	93
	Property sets are a shortcut . . . . .	96
	Reviewing and activating your configuration changes . . . . .	96

<b>Chapter 9</b>	Accounts . . . . .	99
	There are four pre-installed accounts . . . . .	100
	How many people can use Network Discovery at once . . . . .	100
	How the types of accounts differ . . . . .	100
	Creating accounts . . . . .	102
<b>Chapter 10</b>	Backup and Restore . . . . .	107
	About external backups . . . . .	108
	Choosing tape or an FTP site for your external backup . . . . .	109
	Configuring an external backup . . . . .	110
	Testing your external backup and restore. . . . .	111
	To run an internal or external backup immediately . . . . .	112
	Restoring your data . . . . .	113
<b>Chapter 11</b>	To Migrate from InfraTools Network Discovery or from Xanadu . . . . .	117
	How it works . . . . .	118
	Configure your corporate firewall . . . . .	119
	Upgrade the license on your new appliance . . . . .	120
	Ensure that you have a backup from your old appliance . . . . .	120
	Restore the old data to the new appliance. . . . .	121
	You can keep your IND 4 style Seeds, Blocks and Forces . . . . .	122
<b>Chapter 12</b>	Before you call... . . . . .	123
	Overview . . . . .	124
	Check that your maintenance license is current . . . . .	124
	Check that you have the latest software components . . . . .	124
	Download the new component(s) . . . . .	125
	Install the new component(s) . . . . .	125
	After you install new components . . . . .	125
<b>Appendix A</b>	Security Checklist . . . . .	127
<b>Appendix B</b>	Extra Hardware . . . . .	131
	Uninterruptible Power Supply (UPS) units . . . . .	131
	Tape Drive . . . . .	133
	External Modem . . . . .	133

Adding a CPU or a modem later. . . . .	133
Index . . . . .	135







# Preparing for Installation

---

**SECTION**



# 1

## CHAPTER

# Welcome to Network Discovery

---

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.

This information in *Preparing for Installation* is critical to your success with Peregrine’s Network Discovery. Your sales representative may have given it to you as a separate pre-purchase handout; or you may be seeing it for the first time as the first three chapters of the *Network Discovery Setup Guide*. The information is exactly the same. If you have seen the information before and have already done the preparation, you can go to Chapter 4, *Install and Start Network Discovery*. If you are seeing this information for the first time, let’s get started.

---

**Important:** If you are migrating from InfraTools Network Discovery (IND) 4.2 or 4.3, see chapter 11 *To Migrate from InfraTools Network Discovery or from Xanadu* on page 117 of the *Network Discovery Setup Guide*. Instructions for upgrading from Network Discovery 5.0 or 5.0.1 are in the 5.0.2 *Release Notes*.

---

# About Network Discovery

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.

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

ServiceCenter'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.

## Why it's important to prepare

Setting up Network Discovery is quick and easy, provided you properly prepare your network, and use the specified equipment for the Peregrine appliance and the management workstation.

To operate correctly, Network Discovery needs a constant supply of accurate data. To ensure that Network Discovery knows where and how to collect that data, 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.

## Start by collecting information about your network

The next chapter is a questionnaire designed to help you gather information about your network. If you have already filled out this form and sent it in to Peregrine Systems Customer support, collecting all the information is done. Keep the completed questionnaire handy.

The questionnaire is designed to make the setup and use of Peregrine Network Discovery as smooth as possible. Please answer all questions. Peregrine Systems recognizes that some information may be considered secure or private, but providing the information will allow us to create the optimal inventory and management environment. If you need help filling out the questionnaire, please contact your Peregrine or OEM/VAR (Original Equipment Manufacturer or Value Added Reseller) sales representative or contact Peregrine Systems Inc.

Current details of local Peregrine Systems Customer Support offices are available through Peregrine's CenterPoint Web site at <http://support.peregrine.com>.

To find Peregrine worldwide contact information:

- 1 Log on with your login user name and password.
- 2 Click **Go for CenterPoint**.
- 3 Select **Whom Do I Call?** in the navigation bar on the left side of the page. Peregrine worldwide information is displayed for all products.

You can obtain a copy of the questionnaire:

- in a copy of *Preparing for Installation* from your OEM/VAR or Peregrine account representative
- by downloading an Adobe Acrobat PDF copy of *Preparing for Installation* from the CenterPoint web site at [support.peregrine.com](http://support.peregrine.com). (Click **My Products** > **Automation** > **PND**.)
- by printing or photocopying the next chapter

When you have completed the questionnaire, send it to Peregrine Systems Inc. by e-mail, mail or by fax. To find the mailing address or fax number of the Peregrine office in your region, contact your OEM/VAR or check <http://support.peregrine.com>.



# 2 Pre-setup Questionnaire

CHAPTER

## Your contact information

Your Name

---

Organization

---

Address

---

---

---

Telephone

---

E-mail

---

Fax

---

---

## Describe your network's node and subnet setup

Enter the following information to help determine the scale of your network.

**Note:** Network Discovery defines a node as any network device with at least one MAC address. A managed device is a network device that has an SNMP agent and MIB so it can respond to SNMP requests.

How many nodes do you believe are active on your network? \_\_\_\_\_

Are there any remote sites to be managed? Yes \_\_\_\_\_ No \_\_\_\_\_

If yes, approximately how many managed nodes are at remote sites? \_\_\_\_\_

Is your network divided into subnets? Yes \_\_\_\_\_ No \_\_\_\_\_

If yes, how many subnets does your network contain? \_\_\_\_\_

## Enter the Peregrine appliance network information

Enter the information that you will assign to the Peregrine appliance at startup.

**Note:** You will give this IPv4 address to new users so they can log in easily.

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

Planned IPv4 address for your Peregrine appliance \_\_\_\_\_

Subnet mask address \_\_\_\_\_

Default gateway IP address \_\_\_\_\_



## Peregrine Systems Customer Support access

Information on the options you have for receiving Customer Support is in *Choose how to receive Peregrine Systems Customer Support* on page 24.

If you will use a modem and a dedicated analog telephone line, enter the number of the telephone line.

Telephone number for access by  
Peregrine Systems Customer Support

---

## List IPv4 ranges for Network Discovery to discover

Network Discovery uses IPv4 ranges to discover the devices in your network. It 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.

**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.

Please add the IPv4 ranges you want Network Discovery to discover in your network. For example, to discover an entire class C subnet with subnet mask 255.255.255.0 enter an IP range from xxx.xxx.xxx.0 to xxx.xxx.xxx.255 such as 172.17.1.0. to 172.17.1.255. If you require more space, please attach additional sheets as needed.

---

**Important:** When you assign IPv4 ranges, be aware of the size of the ranges you are requesting. If you request a large range of IPv4 addresses to sweep, it can take several hours or days.

---

	From	To
IPv4 range 1		
IPv4 range 2		
IPv4 range 3		
IPv4 range 4		
IPv4 range 5		
IPv4 range 6		

## List IPv4 ranges for Network Discovery to avoid

If there are subsets of the above IPv4 ranges that you do not want Network Discovery to discover, enter them here.

---

**Important:** You do not need to enter ranges outside the ranges you have specified. Network Discovery does not discover ranges unless you specify them.

---

	From	To
IPv4 range 1		
IPv4 range 2		
IPv4 range 3		
IPv4 range 4		

## List the community strings of your network's devices

For an explanation of community strings, see *About community strings* on page 23.

This is a list of non-directed community strings. Directed community strings are covered later.

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, the owner of an Administrator account will be able to manage the device from the Network Discovery interface.

		Rights granted	
Community string	Associated device /IPv4 range	Read	Write

## Enter TCP/IP configuration

The Peregrine appliance must have its own static IP address, but it can manage devices with either static or dynamic IP addresses. Please enter the following information to show how the devices on your network receive IP addresses.

Are TCP/IP addresses static or dynamic?

Static \_\_\_\_\_ Dynamic \_\_\_\_\_

If dynamic, enter the following:

— The IPv4 address(es) of Dynamic Host Configuration Protocol (DHCP) server(s)

\_\_\_\_\_

\_\_\_\_\_

— The DHCP IPv4 address lease time (Peregrine Systems recommends a lease time of at least 7 days.)

\_\_\_\_\_

Is SNMP management enabled on the DHCP server?

Yes \_\_\_\_\_ No \_\_\_\_\_

**Tip:** Enable SNMP management on the DHCP server so that Network Discovery can poll DHCP for the current IP and MAC address pair information of the devices on your network.

**Note:** Please list the IP addresses of any routers you want Network Discovery to monitor, that do not have SNMP management enabled now and will not have management enabled in the future (for example, a router controlled by an Internet Service Provider).

Unmanaged router number 1 \_\_\_\_\_

Unmanaged router number 2 \_\_\_\_\_

Unmanaged router number 3 \_\_\_\_\_

## What server will you use for the Peregrine appliance?

Please check one (for more information, see *Check the server that will be the Peregrine appliance* on page 28):

Large IBM xSeries 335 \_\_\_\_\_

Small IBM xSeries 335 \_\_\_\_\_

Large IBM xSeries 330 \_\_\_\_\_

Small IBM xSeries 330 \_\_\_\_\_

## Send the questionnaire

When you have completed the questionnaire, send it to Peregrine Systems Inc. by e-mail, mail or by fax. To find the mailing address or fax number of the Peregrine office in your region, contact your OEM/VAR or check <http://support.peregrine.com>.

Current details of local Peregrine Systems Customer Support offices are available through Peregrine's CenterPoint Web site at <http://support.peregrine.com>.

To find Peregrine worldwide contact information:

- 1 Log on with your login user name and password.
- 2 Click **Go for CenterPoint**.
- 3 Select **Whom Do I Call?** in the navigation bar on the left side of the page. Peregrine worldwide information is displayed for all products.



# 3 Prepare the network

## CHAPTER

Topics in this chapter include:

- *Turn on SNMP management in all routers and core switches on page 22*
- *Set DHCP lease time on page 22*
- *(Optional) Turn on SNMP management in other devices on page 23*
- *About community strings on page 23*
- *Give the Peregrine appliance IP address to all devices using directed community strings on page 23*
- *(Optional) Adjust bridge aging on page 24*
- *Plan the device and port to which the Peregrine appliance will be attached on page 24*
- *Choose how to receive Peregrine Systems Customer Support on page 24*
- *Enable firewall ports on page 26*
- *Check Cisco devices on page 28*
- *Check Committed Information Rate (CIR) values on page 28*
- *Check the server that will be the Peregrine appliance on page 28*
- *Check the management workstation on page 31*

## Turn on SNMP management in all routers and core switches

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. The more managed devices in your network, the better. However, enable switches and routers first.

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

What if you don't turn on SNMP management in your switches and routers?

- Network Discovery will appear to work, but you'll eventually notice that it is working poorly. Once Network Discovery is up and running, the Exceptions reports can advise you of problems. Much of the information that Network Discovery collects comes from the SNMP MIB of devices in your network, so it is crucial that you enable SNMP management.

How do you turn on SNMP management?

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

**Note:** When you turn on SNMP management in a device, you often assign a community string. If you assign a new string later, be sure you give the community string to the Peregrine appliance. For more information, see *About community strings* on page 23.

## Set DHCP lease time

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.



## (Optional) Turn on SNMP management in other devices

Your decision to turn on SNMP management in your remaining switches, hubs, servers and workstations depends on the results you expect from Network Discovery. For example, in many networks, monitoring the performance of workstations is not important.

### About community strings

A community string is like a password. A device uses a community string to protect its SNMP MIB—and it's the data from the SNMP MIB that Network Discovery relies on. Network Discovery must know at least one of a device's passwords to collect data from that device. If you do not give Network Discovery a device's community string, Network Discovery will behave as though the device does not have SNMP management turned on. Network Discovery will appear to work, but you'll eventually notice that it is working poorly. Once Network Discovery is up and running, the Exceptions reports can advise you of problems.

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

#### Directed community strings

Directed community strings give devices another layer of protection: a list of IP addresses of approved devices. When Network Discovery tries to get information from a device with a directed community string, the device asks not only “What's the password?” but also “Are you on the list?”

## Give the Peregrine appliance IP address to all devices using directed community strings

When directed community strings are used, it is not enough to give Network Discovery access to the device. You must also configure the device to recognize the Peregrine appliance. You must put it on the list of approved devices.

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

- Network Discovery will behave as though the device does not have SNMP management turned on. Network Discovery will appear to work, but you'll eventually notice that it is working poorly. Once Network Discovery is up and running, the Exceptions reports can advise you of problems.

## (Optional) Adjust bridge aging

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. Network Discovery's Exceptions reports can tell you which devices should have their bridge aging adjusted.

## Plan the device and port to which the Peregrine appliance will be attached

Plan to attach the Peregrine appliance:

- behind your corporate firewall
- to an Ethernet port on a device close to the top of your network. Network Discovery works best if the port is SNMP managed.

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

## Choose how to receive Peregrine Systems Customer Support

Options for allowing Customer Support access (in the order in which Peregrine Systems recommends them) are as follows:

- through Internet access
- through a Virtual Private Network over Internet

- by a modem and a dedicated analog telephone line
- through a Remote Access Server (RAS)

## Through Internet access

For you to have Customer Support by means of the Internet you must enable certain ports in the corporate firewall. Peregrine Systems Customer Support requires access for the following IP address: 209.167.240.9 (sprocket.loran.com).

**Table 3-1: Firewall ports to enable for Customer Support**

Used for	Port	Note
Secure Shell (SSH)	22/tcp	
HTTP	80/tcp	
MIB browser	8100/tcp	
Network Map	8101/tcp	
Network Map proxy	8102/tcp	1,2
MIB browser proxy	8103/tcp	1
Telnet proxy	8104/tcp	1
HTTP proxy	8105/tcp	1
MySQL ODBC	8108/tcp	
<b>Note:</b>		
1. Depending on your settings for Appliance proxy services		
2. If you have an Aggregator license		

## Virtual Private Network over the Internet

Contact Peregrine Systems Customer Support to send them the software that will enable access. If you have a firewall, enable the firewall ports listed in the above table, *Firewall ports to enable for Customer Support*.

## By modem and dedicated telephone line

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). An internal modem and an analog telephone line allow you to have access to Customer Support even when you cannot use the Internet.

**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.)

Instructions for purchasing a modem and attaching the hardware are in chapter 4, *Install and Start Network Discovery* on page 35.

## Through a Remote Access Server (RAS)

Contact Peregrine Systems Customer Support to send them the IP address or telephone number that will enable access. If you have a firewall, enable the firewall ports listed in the above table, *Firewall ports to enable for Customer Support*.

## Enable firewall ports

Enabling these firewall ports is not just to allow access to Customer Support on the Internet; it is to enable any Network Discovery system to perform through a corporate firewall.

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

Table 3-2: Firewall ports to enable for Network Discovery to perform

Used for	Port	Note	From	To
Secure Shell (SSH)	22/tcp		Peregrine Systems Customer Support	Peregrine appliance
Telnet	23/tcp	1	Peregrine appliance	device
		1	management workstation	device
SMTP	25/tcp		Peregrine appliance	SMTP server
DNS	53/udp		Peregrine appliance	DNS server
HTTP	80/tcp		management workstation	Peregrine appliance
		1	management workstation	device
		1	Peregrine appliance	device
		2	Peregrine appliance	aggregated Peregrine appliance
NTP (network time)	123/udp		Peregrine appliance	NTP server
NetBIOS-n (name server)	137/udp		Peregrine appliance	device
NetBIOS-dgm (datagram)	138/udp		management workstation	Peregrine appliance
NetBIOS-ssn (session—file and printer sharing)	139/tcp		management workstation	Peregrine appliance
SNMP	161/udp		Peregrine appliance	device
SNMP traps	162/udp	3	Peregrine appliance	external network management server
MIB Browser	8100/tcp		management workstation	Peregrine appliance
		2	Peregrine appliance	aggregated Peregrine appliance
Network Map	8101/tcp		management workstation	Peregrine appliance
		2	Peregrine appliance	aggregated Peregrine appliance
Network Map proxy	8102/tcp	2	management workstation	Peregrine appliance
MIB browser proxy	8103/tcp	2	management workstation	Peregrine appliance

Telnet proxy	8104/tcp	1	management workstation	Peregrine appliance
		1,2	Peregrine appliance	aggregated Peregrine appliance
HTTP proxy	8105/tcp	1	management workstation	Peregrine appliance
		1,2	Peregrine appliance	aggregated Peregrine appliance
MYSQL ODBC	8108/tcp	1	management workstation	Peregrine appliance
Traceroute	33263/udp		Peregrine appliance	device
<b>Note:</b>				
<ol style="list-style-type: none"> <li>1. Depending on your settings for Appliance proxy services</li> <li>2. If you have and Aggregator license</li> <li>3. If you are using SNMP trap notification</li> </ol>				

## 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 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.

## Check the server that will be the Peregrine appliance

You must install the Network Discovery software onto a server meeting the following hardware requirements.

For a new installation, use an IBM xSeries 335.

You can also upgrade an existing Network Discovery installation on an IBM xSeries 330 that meets the following hardware requirements.

**Note:** Failure to meet the hardware requirements described in the following tables will result in Network Discovery not installing.

**Table 3-3: Summary of IBM servers certified for Network Discovery**

For a large Peregrine appliance (managing up to 10,000 devices)	For a small Peregrine appliance (managing up to 5,000 devices)
IBM xSeries 335, 1 CPU, 2GB RAM with two 36 or 73GB SCSI disks	IBM xSeries 335, 1 CPU, 1GB RAM, with two 36 or 73GB SCSI disks
IBM xSeries 330, 2 CPUs, 2GB RAM, with two 36 or 73GB SCSI disks	IBM xSeries 330, 1 CPU, 1GB RAM with two 36 or 73GB SCSI disks

**Table 3-4: Specific IBM xSeries 335 hardware requirements**

Part Number	Part Description	Qty	Approved Supplier	Remarks
8676-61x	CPU IBM xSeries 335 with 1 Xeon 2.4 GHz or better processor  Level 2 512KB full-speed cache per processor  1 or 2GB RAM	1	IBM	Approved server. Manufacturer may install better system processor      On the IBM xSeries 335 you will need 1 or 2 GB RAM depending on how many devices you wish to manage
IGM-PCI 56k/LD	56KB PCI Data/Fax modem (internal)	1	Buffalo/Melco	PCI-X 3.3 V; based on Conexant modem chip (Optional) Required to receive customer support by telephone line.
06P4792	C2T Cable Kit	1	IBM	Contains the C2T breakout cable that enables you to connect a monitor and keyboard to the server

Part Number	Part Description	Qty	Approved Supplier	Remarks
	keyboard	1		A USB keyboard is not supported. The keyboard is only required at startup, to access the configuration interface
	monitor	1		The monitor is only required at startup, to access the configuration interface

**Table 3-5: Specific IBM xSeries 330 hardware requirements**

Part Number	Part Description	Qty	Approved Supplier	Remarks
867441x	CPU IBM xSeries 330 with one or two Pentium III 1.4 GHz or better processors  Level 2 512KB full-speed cache per processor  1 or 2GB RAM	1 or 2	IBM	Approved server. Manufacturer may install better system processor       On the IBM xSeries 330 you will need one processor and one GB RAM to manage up to 5,000 devices. You will need two processors and two GB RAM to manage up to 10,000 devices.
33L4618	56KB PCI Data/Fax modem (internal)	1	IBM	Only use IBM modem (Optional) Required to receive customer support by telephone line.
06P4792	C2T Cable Kit	1	IBM	Contains the C2T breakout cable that enables you to connect a monitor and keyboard to the server
	keyboard	1		A USB keyboard is not supported. The keyboard is only required at startup.
	monitor	1		The monitor is only required at startup.



## Check the management workstation

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

**Table 3-6: Requirements and recommendations for the management workstation**

Item	Required	Recommended
Web browser	Use Netscape 4.07 or later (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 <sup>a</sup>	Internet Explorer 5.0 or later
Video		
—colors	256 <sup>b</sup>	65,000 or more
—resolution	800×600	1024×768 or more
Memory (MB RAM)	32 <sup>c</sup>	64 <sup>d</sup> or more
CPU	Pentium 100 equivalent	Pentium II 233 equivalent or better
Operating system		Windows 2000 or better

a Requires a Virtual Machine (VM) upgrade.

b 256 colors normally give adequate performance. However, in Netscape (with Windows 95, Windows 2000, or Windows NT), there may be unexpected colors on the Network Map.

c You must close all applications other than your web browser.

d 128 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:

<b>Browser</b>	<b>Java Environment</b>
Internet Explorer 5.0	Native only
Internet Explorer 5.5	Native or JRE 1.4.1
Internet Explorer 6.0	Native or JRE 1.4.1
Netscape 4.x	Native only
Netscape 6.2 and 7.0	JRE 1.4.1



# Installation

---

**SECTION**



# 4 Install and Start Network Discovery

## CHAPTER

This chapter describes how to install Network Discovery software on the server and how to install the server in your network.

Topics in this chapter include:

- *About installing the hardware on page 36*
- *Connect a keyboard and monitor directly to the Peregrine appliance on page 36*
- *Set the BIOS boot sequence on page 37*
- *Install Network Discovery software from the CD on page 38*
- *Give the Peregrine appliance its network information on page 39*
- *Connect the server to the network on page 43*
- *Connect a management workstation to the network on page 44*
- *Connect an Uninterruptible Power Supply (UPS) on page 45*
- *(Optional) Connect the Peregrine appliance to a telephone line on page 46*
- *Connect data backup equipment and pager hardware on page 45*
- *(Optional) Connect the Peregrine appliance to a telephone line on page 46*
- *Connect the Peregrine appliance to AC power on page 46*

## About installing the hardware

When you install the server, follow the server installation documentation. The server installation documentation may vary depending on what version of server you have. The server installation documentation was included in the shipping box. If the documentation is missing or you have a problem, contact the hardware manufacturer.

## Connect a keyboard and monitor directly to the Peregrine appliance

You need a keyboard and monitor to communicate directly with the server so that you can use the configuration interface to get Network Discovery installed and up and running. The configuration interface is used when you cannot access Network Discovery by means of your web browser.

You will not need the keyboard and monitor after Network Discovery is up and running, unless you need to access the configuration interface again.

You can install the server that will act as your Peregrine appliance in its permanent location now or you can do the software work first and then detach the keyboard and monitor before moving the Peregrine appliance to its permanent location.

---

**Important:** A USB keyboard is not supported.

---

The following instructions are for any IBM eserver xSeries versions of the Peregrine appliance.

### To attach 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.
- 3 Follow your server installation documentation to connect the AC power and turn the server on.

## Set the BIOS boot sequence

You must configure the BIOS of the Network Discovery server to use the correct boot sequence. (There are slight differences between the procedures for the IBM xSeries 335 and the IBM xSeries 330).

### To set the BIOS boot sequence

After you power the server on, wait until the display shows **Press F1 for Configuration/Setup**.

**1** Press **F1**

You see the Configuration/Setup/Utility menu.

**2** Use the arrow keys to select **Load Default Settings** and press **Enter**

**3** Press **Enter** again.

You return to the Configuration/Setup Utility main menu. If you have an IBM xSeries 335, continue with all of the steps. If you have an IBM xSeries 330, go to step 8.

**4** Use the arrow keys to select **Start Options** and press **Enter**

**5** Press **Enter** again.

**6** Verify that the options are set as follows. Do not change options that are not listed here. Use the arrow keys to make changes.

Planar Ethernet PXE/DHCP	Disabled
Disketteless Operation	Enabled
Displayless Operation	Enabled
Keyboardless Operation	Enabled
Boot on Post/BIOS Error	Enabled

**7** Press **Esc**

You see the Configuration/Setup Utility main menu again.

**8** Use the arrow keys to select **Start Options** and press **Enter**

**9** Use the arrow keys to select **Startup Sequence Options** (IBM xSeries 335) or **Startup Sequence** (IBM xSeries 330) and press **Enter**.

**10** Verify that the options are set as follows. Do not change options that are not listed here. Use the arrow keys to make changes.

First Startup Drive	CD ROM
Second Startup Drive	Hard Disk 0

- Third Startup Drive                      Diskette Drive 0
- 11 Press **Esc** twice to return to the Configuration/Setup Utility main menu.
  - 12 Use the arrow keys to select **Save Settings** and press **Enter**
  - 13 Press **Enter** again.  
You see the Configuration/Setup Utility main menu again.
  - 14 Use the arrow keys to select **Exit Setup** and press **Enter**.
  - 15 Press **Enter** again to reboot the system, so you can go on to install the Network Discovery software.

## Install Network Discovery software from the CD

The installation of Network Discovery is automated and requires very little user intervention.

To install the Network Discovery software, you need the following:

- A system server as specified in *Check the server that will be the Peregrine appliance* on page 28. All of the hardware components must be installed before the Network Discovery software is installed.
- A Network Discovery installation CD.
- A monitor and PS2 keyboard attached to the server.

---

**Important:** A USB keyboard is not supported.

---

To install Network Discovery:

- 1 Place the Network Discovery installation disc in the CD-ROM drive of the server and restart the server.

The system boots from the CD and then prompts you to enter one of two options:

- reformat (reformats the hard disks to factory specifications)
- boot (reboots the system)

- 2 Type reformat and press **Enter**.

After the format has completed, you see the options again:

- reformat
- boot



- 3 Type **boot** and press **Enter** to restart the system.

During the reboot, the installation CD detects that the hard drives are formatted correctly and installs the packages required for Network Discovery. After the packages have been installed, the CD ejects, and the server reboots.

- 4 Remove the CD and store it in a safe place.

Network Discovery is installed on the server and you now have a Peregrine appliance.

If you see an error message telling you that there is a problem with the hardware, contact Peregrine Systems Customer Support.

## Give the Peregrine appliance its network information

Working with the configuration interface, you will enter the IPv4 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 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.

- 3 Press **Enter**

### To use the configuration interface to give the Peregrine appliance its network information

The screen shows the Appliance Management menu:

- 1) Settings
- 2) Actions
- 3) Appliance hardware information
- 4) Exit and log off

- 1 Type 1 (or use the arrow keys to move the cursor to 1) and press **Enter**

The screen show the Appliance Settings menu:

- 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

- 2 Type 2 and press **Enter**

The screen shows the IP Networking menu:

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

- 3 Type 3 and press **Enter**

- 4 Type the IP address of the Peregrine appliance.

- 5 Press **Enter**

- 6 Type 4 and press **Enter**

- 7 Type the netmask of the Peregrine appliance.

- 8 Press **Enter**

- 9 Type 5 and press **Enter**

- 10 Type the gateway of the Peregrine appliance.

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

- 11 Press **Enter**

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

- 12 Type 6 and press **Enter**

- 13 Wait briefly.

---

**Important:** While you're waiting, change the Peregrine appliance's default password for security.

---

### To change the Peregrine appliance's default password

On the IP Networking menu:

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

**1 Press 1 and press Enter**

The screen shows the Appliance Settings menu:

- 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

**2 Type 10 and press Enter**

**3 Follow the screen prompts.**

**4 When you have retyped your new password, press Enter.**

The screen shows the Appliance Settings menu.

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

### To complete the installation

► **Type 1 and press Enter**

The screen shows the Appliance Management menu:

- 1) Settings
- 2) Actions
- 3) Appliance hardware information
- 4) Exit and log off

If the Peregrine appliance is in its permanent location, type 4 to exit and log off.

If you have not yet installed the Peregrine appliance in its permanent location, do the following:

- shut the Peregrine appliance down (see *To shut down the Peregrine appliance—through the configuration interface* below)

---

**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.

---

- disconnect the AC power
- remove the keyboard, monitor and C2T breakout cable
- and install the Peregrine appliance in its final location, following the instructions from *About installing the hardware* on page 36.

**To shut down the Peregrine appliance—through the configuration interface**

---

**Warning:** Do not shut down the Peregrine appliance during the procedure to give the Peregrine appliance its network information, unless you need to abandon the procedure.

---

The Appliance Management menu shows:

- 1) Settings
- 2) Actions
- 3) Appliance hardware information
- 4) Exit and log off

1 Type 2

The screen shows the Appliance Actions menu:

- 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 to confirm that you want to shut down the Network Discovery server.  
When the screen shows: “The system is halted”...
- 4 Power off the Peregrine appliance.  
The Peregrine appliance shuts down safely.

## Connect the server to the network

### Top-of-the-network device

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

---

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

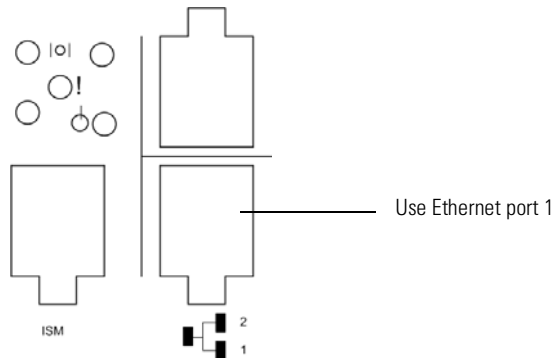
---

The port that allows the Peregrine appliance access to the network must be Ethernet. Network Discovery automatically detects what speed the Ethernet port is and whether it is full- or half-duplex. Network Discovery works best if the port is SNMP managed.

## IBM xSeries 335 Peregrine appliance

On the IBM xSeries 335 Peregrine appliance, connect the top-of-the-network device to the Peregrine appliance's Ethernet port 1, the bottom right port.

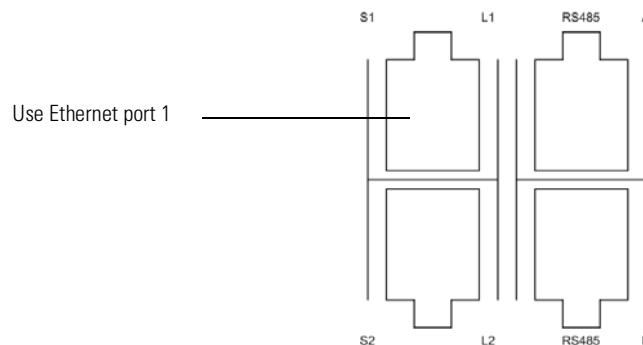
Figure 4-1: IBM xSeries 335 ports



## IBM xSeries 330 Peregrine appliance

On the IBM xSeries 330 Peregrine appliance, connect the top-of-the-network device to the Peregrine appliance's Ethernet port 1, the top left port.

Figure 4-2: IBM xSeries 330 ports



## Connect a management workstation to the network

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

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 or outages. Having the management workstation connected to the same concentrator or switch as the Peregrine appliance also ensures that the management workstation does not become isolated from Network Discovery in the event of device failures.

## 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 131.

---

**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 warnings* on page 69.

## 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 107.

For tape drive requirements, see *Appendix B, Extra Hardware* on page 131.

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.

## (Optional) Connect the Peregrine appliance to a telephone line

Connect the to a telephone line, if you have chosen a telephone and modem as your means of receiving customer support. (For other options, see *Choose how to receive Peregrine Systems Customer Support* on page 24).

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.

## Connect the Peregrine appliance to AC power

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

## Optional use of terminal emulation software

You can use an RS-232 serial cable to connect a terminal or a workstation running terminal emulation software instead of the keyboard and monitor any time you need to access the configuration interface—with one exception. You must use a keyboard and monitor to change the BIOS (see *Set the BIOS boot sequence* on page 37).



To use a terminal or a workstation running terminal emulation software

- 1 Use an RS-232 serial cable to 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 4-1: Terminal requirements or settings**

<b>Item</b>	<b>Requirement</b>
Speed	9600
Bits	8
Parity	None
Stop Bits	1
Terminal type	vt100



# 5 Appliance Management

## CHAPTER

Some of the tasks in this chapter are optional.

Topics in this chapter include:

- *Log in to Network Discovery* on page 50
- *How to shut down the Peregrine appliance* on page 53
- *The Home page* on page 53
- *The Toolbar* on page 54
- *Assign a system name, contact, and location* on page 57
- *Change the Peregrine appliance community strings* on page 57
- *Set the time zone* on page 58
- *Enter the domain name server* on page 59
- *Enter the host name* on page 61
- *Enter the Workgroup name* on page 62
- *Enter the Administrator e-mail address* on page 63
- *Enter the SMTP server* on page 63
- *Set the system time* on page 65
- *Change the default Admin password* on page 68
- *About disabling warnings* on page 69

# 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 5-1: 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 lowercase.

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 one or more security warnings. 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, 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 68.

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 through the configuration interface (*Give the Peregrine appliance its network information* on page 39). You can go back, re-attach the keyboard and monitor, and check the network information.
- If the network 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.
- Check that you connected the Ethernet cable to the correct Ethernet port (see *Connect the server to the network* on page 43)
- 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. There are two possibilities:

- Your browser has JavaScript turned off.
- You have pop-up windows disallowed (for instance in a software plug-in or in Netscape 6 or 7 **Edit > Preferences**).

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.

---

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

---

**Warning:** Do not shut down the Peregrine appliance during the procedure to give the Peregrine appliance its network information, unless you need to abandon the procedure.

---

**Note:** To shut down the Peregrine appliance safely when you are using the configuration interface, see *To shut down the Peregrine appliance—through the configuration interface* on page 42.

To shut down the Peregrine appliance—through the browser interface

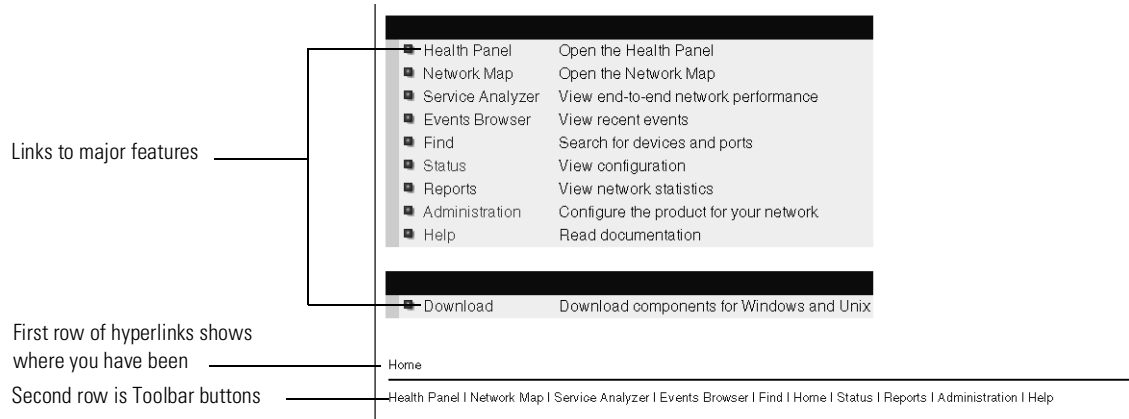
- 1 **Administration > Appliance Management > Appliance Shutdown**
- 2 **Click Shut down appliance.**  
When the screen shows: “The system is halted”...
- 3 **Power off the Peregrine appliance.**  
The Peregrine appliance shuts down safely.

## 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, it provides an opportunity to introduce the navigation hyperlinks. Two rows of 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 5-1: 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 5-2: Toolbar**



## The banner or title bar




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










## The buttons

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

- Point to a button with your cursor and hold down your mouse button to see labels (mini-help messages).

**Table 5-2: Toolbar buttons**

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.
- Loading progress messages appear when Network Discovery is loading the Main Map and the Health Panel.

## Assign a system name, contact, and location

- “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 Network Discovery Administrator.
- “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 250 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 or refresh the Toolbar (F5).

## Change the Peregrine appliance community strings

We recommend that you:

- change the Peregrine appliance’s read-only string to the one used by the rest of the devices in your network. The read-only community string allows read access to the Peregrine appliance MIB.
- change the Peregrine appliance’s read/write community string (for security reasons). The read/write community string allows read and write access to the Peregrine appliance MIB

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

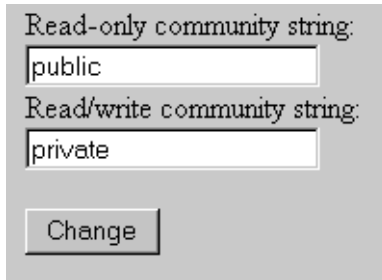
There is more information on community strings in:

- *About community strings* on page 23
- *Add community strings—the quick way* on page 79
- *More on community strings* on page 93.

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 5-3: 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 you first configure 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.

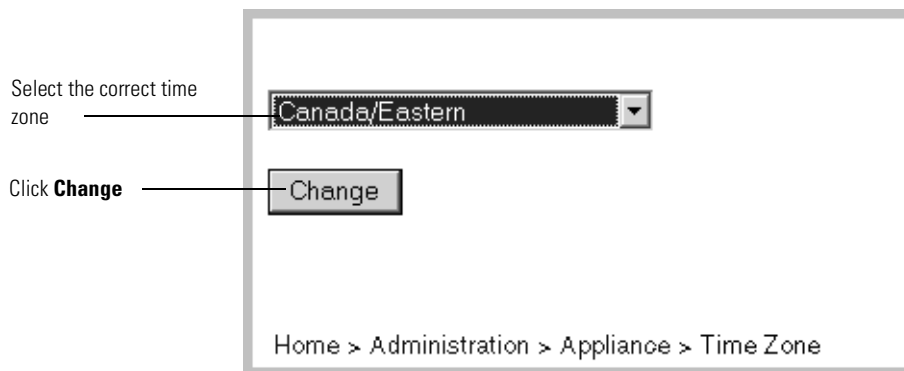
---

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 5-4: 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.
- 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. 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 5-5: Change domain name server**

Enter DNS so that domain names will appear on map windows, reports and so on

Enter order Network Discovery should use to complete a domain name

Domain name servers (IPv4 addresses):  
192.168.133.1

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

Change

Home > Administration > Appliance > Domain Name Servers

## 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 5-6: Change 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 a shared directory into which you can deposit:

- license files when you download them from the Peregrine Customer Support web site
- updated software components
- 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.

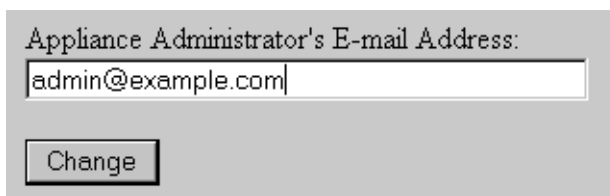
---

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 5-7: Enter e-mail address**



Appliance Administrator's E-mail Address:

## 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 SMTP 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).

---

**Important:** Peregrine Systems recommends that you use a local SMTP server. 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.

---

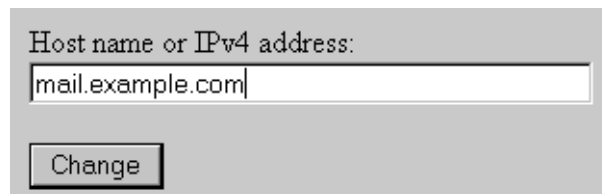
**Note:** Use the IPv4 address rather than the domain name of the SMTP server so that Network Discovery can still contact you even if the domain name server is unavailable.

**Note:** Setting up the SMTP server and supplying an e-mail address are two separate tasks. If you do not supply a 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 5-8: Change SMTP server**



Host name or IPv4 address:

## Set the system time

Network Discovery uses the system time to monitor your network, to generate reports, and to adjust to daylight savings time automatically.

Perform one of the two following procedures, not both.

- *Set the date and time*, next section
- *Synchronize the time* on page 66 (or *Enter an NTP server to synchronize the time (continually)* on page 67)

## 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 66).
- 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 5-9: Setting the time and date

Year:

Month:

Day:

Hours:  (0-23)

Minutes:

Home > Administration > Appliance > Set Time

## 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.

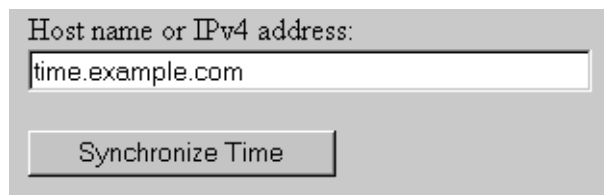
**Note:** The Synchronize Time option only synchronizes the time once. It does not repeatedly re-synchronize.

To synchronize the time

- 1 Make sure the time zone is set (see *Setting the time and date* on page 66).
- 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**.

The time is now the same as the server you synchronized with, but the times may diverge later.

**Figure 5-10: Synchronize time**



A screenshot of a web interface for synchronizing time. It features a text input field labeled "Host name or IPv4 address:" containing the text "time.example.com". Below the input field is a button labeled "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**.

The time is now the same as the time on the NTP server and it will stay the same.

**Figure 5-11: Change NTP server**



A screenshot of a web interface for changing the NTP server. It features a text input field labeled "Host name or IPv4 address:" containing the text "time.example.com". Below the input field is a button labeled "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 127.

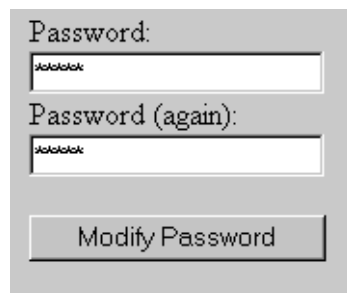
**Note:** When you change the password for the admin account, you will have to log in again. (It is always necessary to log in again when you change the password for the account you are using.)

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 5-12: Changing the admin password**



The image shows a web form for changing the admin password. It consists of two text input fields, one for the new password and one for the confirmation password, both containing masked characters. Below the fields is a button labeled 'Modify Password'.

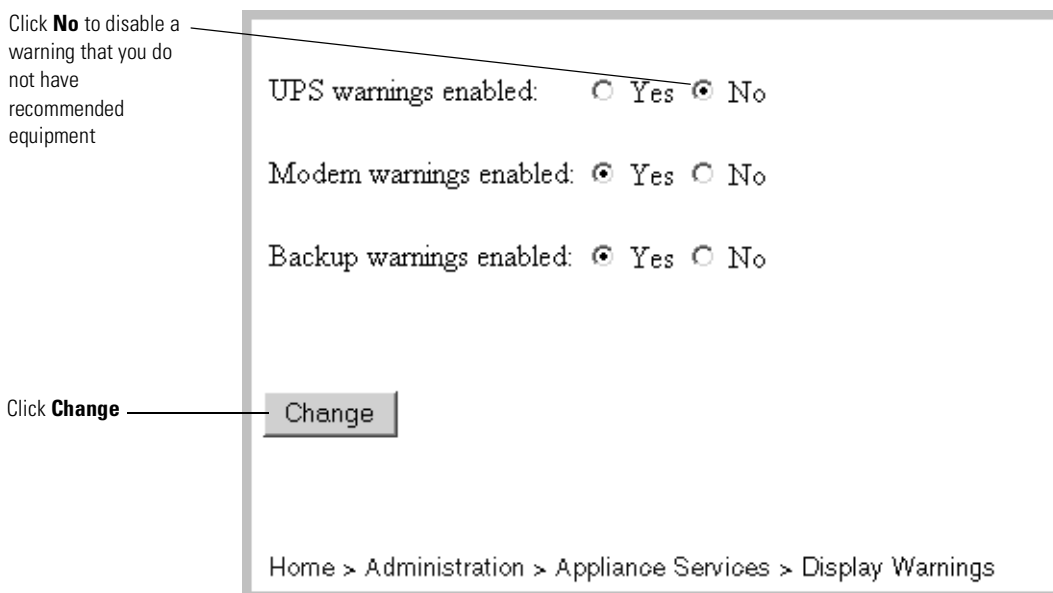
Form fields and button:

- Label: Password:
- Input field: [masked password]
- Label: Password (again):
- Input field: [masked password]
- Button: Modify Password

## About disabling warnings

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

Figure 5-13: Enable or disable warnings



## Disabling UPS warnings

**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**.

## Disabling modem warnings

Network Discovery generates warnings if it does not detect an internal modem. If you have chosen to receive customer support through the Internet, over a Virtual Private Network or over a Remote Access Server, you can disable this modem warning.

To enable or disable the modem warning

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

## Disabling backup warnings

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**.



# 6 Licenses

---

## CHAPTER

Peregrine Systems makes increased functionality available through license files you can download and install.

Topics in this chapter include:

- *How it works* on page 72
- *Request a new license* on page 72
- *Install the new license* on page 73

## 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.

Maintenance contracts entitling you to periods of support from Peregrine Systems Customer Support are also distributed in the form of licenses.

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

## Request a new license

If you purchased Network Discovery from an Original Equipment Manufacturer or a Value-Added Reseller, follow your OEM/VAR's instructions to obtain a license.

If your Peregrine appliance is configured to send e-mail (the instructions were in chapter 5, *Appliance Management* on page 49), you can either send your request directly from the appliance or you can cut and paste the information into an e-mail.

If your Peregrine appliance is not configured to send e-mail, enter the information requested on the form into an e-mail and send it to support@peregrine.com.

To request a license on a Peregrine appliance configured to send e-mail

- 1 **Administration > Appliance Management > Generate licensing request.**

- 2 Complete the form.
- 3 Select **Send e-mail from the appliance to support@peregrine.com** and click **Generate Request**.  
Network Discovery sends your request to Peregrine Systems Customer Support automatically.  
or  
Select **Print out all the information, and I will e-mail it to support**.  
Copy the information into an e-mail and send it 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 Administrator (or IT Manager) account 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 performs the installation.

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

**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 11, *To Migrate from InfraTools Network Discovery or from Xanadu* on page 117 and come back to the next chapter when you are instructed to do so.

# 7 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 Migrate from InfraTools Network Discovery or from Xanadu* on page 117. 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 76
- *Set up the IPv4 range(s) to discover* on page 76
- *Set up the IPv4 range(s) to avoid* on page 78
- *Add ranges for DHCP servers and unmanaged routers* on page 78
- *Add community strings—the quick way* on page 79
- *Activate your proposed changes* on page 80
- *Check that it's working* on page 80

## 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 “DHCP server”). 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 83.

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 Migrate from InfraTools Network Discovery or from Xanadu* on page 117.

---

## 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**.

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 4, 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.

## Add ranges for DHCP servers and unmanaged routers

If you have one or more DHCP servers or you have unmanaged routers, add their IPv4 ranges and apply the appropriate Property Group so that Network Discovery will monitor the ranges differently.

To add IPv4 addresses to be treated as DHCP servers or unmanaged routers

- 1 Click **Administration > Network configuration > Add IPv4 range**.
- 2 Enter the starting and ending IPv4 addresses for the DHCP server or unmanaged router. (Remember if it's a range consisting of one device, the starting and ending IPv4 addresses are the same.)
- 3 For **Property Set/Group**, select one of the default Network Property Groups, **DHCP server** or **Unmanaged router**.

Network Discovery gives the device the properties it should have.

- 4 Click **Submit**.

Repeat steps 1 to 4, if necessary, for all the devices you want Network Discovery to treat as DHCP servers or unmanaged routers.



You have added the range(s) to be treated as DHCP servers and unmanaged routers to your proposed new configuration, but your changes will not take effect until after you have reviewed and activated your changes.

## Add community strings—the quick way

For an explanation of community strings, see *About community strings* on page 23.

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

Here’s how it works. 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).
- 6 Click **Add**.
- 7 Repeat steps 5 and 6 for each of your community strings.
- 8 When you add community strings, the order is important. Are your most frequently used community strings at the top of the list? If necessary, select a community string and click the **Move Up** or **Move Down** button to move it to the right place.
- 9 Click **Submit**.

**Note:** To assign different community strings to different IPv4 ranges, see the next chapter, *Refining Network Discovery* on page 83.

## 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 you proposed 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.

## Check that it's working

There are a couple of things you can do to make sure Network Discovery is up and running properly.

### Are devices appearing on the Network Map?

Within the next few minutes, you can check that network discovery is occurring.

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.

## Are there problems on the Exceptions reports?

Over the next few days, you can check the Exceptions reports for any problems. The Exceptions reports will tell you if and why Network Discovery is having trouble collecting data for example, because a device does not have SNMP management enabled or because Network Discovery needs some community strings.

From now on, check the Exceptions reports regularly, and especially after you make changes.

To check an Exceptions Report

- ▶ Click **Reports > Support > Exceptions Summary** or, on the Health Panel, click the **Exceptions** button.



# 8 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 84*
- *A tree of IPv4 ranges on page 84*
- *Property Groups on page 86*
- *Network Property Groups on page 86*
- *How to use Network Property Groups on page 89*
- *Making changes to Network Property Groups on page 90*
- *Apply a Network Property Group to a range on page 92*
- *Community Property Groups on page 92*
- *More on community strings on page 93*
- *Property sets are a shortcut on page 96*
- *Reviewing and activating your configuration changes on page 96*

## A precise matrix of network discovery

In chapter 7, *Set up Network Discovery* on page 75, there were instructions to set up discovery quickly and simply just to get started. The instructions were basically to apply the Network Property Group, “Active discovery”, to all of your IPv4 range or ranges and give them all the same set of community strings.

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.

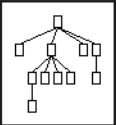
On the other hand, you may decide you want even more information from certain ranges. Perhaps you want to turn on resource management to have disk and CPU information from servers or printers

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.

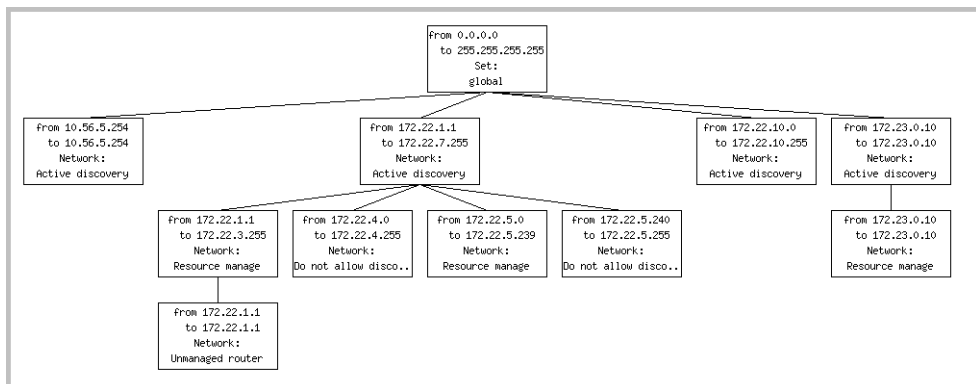
Figure 8-1: Example of a developed network tree as shown in “List IPv4 ranges”

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
--[172.22.5.0 to 172.22.5.239]	Network: Resource manage
--[172.22.5.240 to 172.22.5.255]	Network: Do not allow discovery
--[172.22.10.0 to 172.22.10.255]	Network: Active discovery
--[172.23.0.10 to 172.23.0.10]	Network: Active discovery
--[172.23.0.10 to 172.23.0.10]	Network: Resource manage



Home > Administration > Network Configuration > List

Figure 8-2: Example of a developed network tree as shown in “Review changes”



**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 Click Merge.**

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

## 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 8-3: 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	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	inherit
	Allow IP addresses to accumulate, useful for unmanaged routers									
<u>DHCP server</u>	inherit	inherit	inherit	inherit	on	inherit	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	off	inherit
	Do not allow discovery or add to device model									
<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 manage</u>	on	on	on	inherit	off	off	on	on	inherit	
	Do not apply service management									

## 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:

**Table 8-1: Default Network Properties**

Property	Purpose
Allow devices	Allow devices to be added
Actively ping	Actively ping devices for discovery

Property	Purpose
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	Set to <b>Off</b> when multiple servers have the same IPv4 address that you don't want to see, for instance, when you are using Network Address Translation (NAT). Set to <b>On</b> when you want to allow the repeated IPv4 addresses to be included.
Allow ICMP and SNMP	Although ping and polling is turned off, devices can still be discovered by WMI and included in the database
Device modeler interval	Determines how frequently Network Discovery updates your view of the network. 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 8-2: 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, but does allow IP addresses.
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, <b>Accumulate IP addresses</b> is set to “on”. For routers that do not have SNMP management enabled.
DHCP Server	This Property Group has <b>Force ARP table read</b> 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 8-3: 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	<b>Do not resource manage</b> has the same property values as <b>Active Discovery</b> . Use it as a “child” range of a <b>Resource Manage</b> 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.

## Making changes to Network Property Groups

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**.

## 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.

**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 values to “inherit”.

### 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 apply 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 Network configuration 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 8-4: Default Property Sets**

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

## 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 7. 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”).

Network Discovery also shows you any configuration problems it detects. 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 > Reset to previous configuration**.
- 2 Click **Undo**.



# 9 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 100.*
- *How many people can use Network Discovery at once on page 100.*
- *How the types of accounts differ on page 100.*
- *Creating accounts on page 102.*

## 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 9-1: 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 9-1: What the accounts can do**

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

	Demo	IT Employee	IT Manager	Administrator
SNMP query default string	“public”	“public”	from Network Discovery	from Network Discovery
Update Model	—	—	YES	YES
Configure connections	—	—	YES	YES
Break and force connections	—	—	YES	YES
<b>MIB Browser</b>				
Set SNMP variables	—	—	YES	YES
Read community string	view	view + edit	view + edit	view + edit
Write community string	—	—	view + edit	view + edit
<b>Status</b>				
View read and write community strings for network	—	—	YES	YES
<b>Administration</b>				
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)

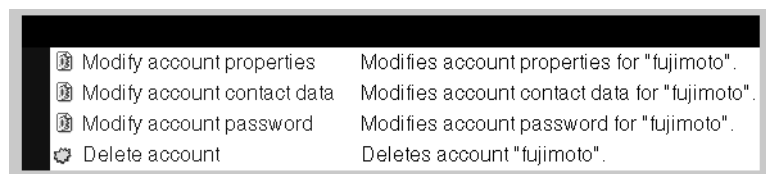
- 3 Click **Add Account**.

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 9-2: 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 9-3: Entering an account password**

The image shows a dialog box for modifying a password. It has two text input fields. The first is labeled 'Password:' and the second is labeled 'Password (again):'. Both fields contain masked characters (asterisks). A callout box with a line pointing to both fields contains the text 'Enter the same password in both boxes'. Below the fields is a button labeled 'Modify 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**.



# 10 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 108
- *Choosing tape or an FTP site for your external backup* on page 109
- *Configuring an external backup* on page 110
- *Testing your external backup and restore* on page 111
- *To run an internal or external backup immediately* on page 112
- *Restoring your data* on page 113

## 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.

---

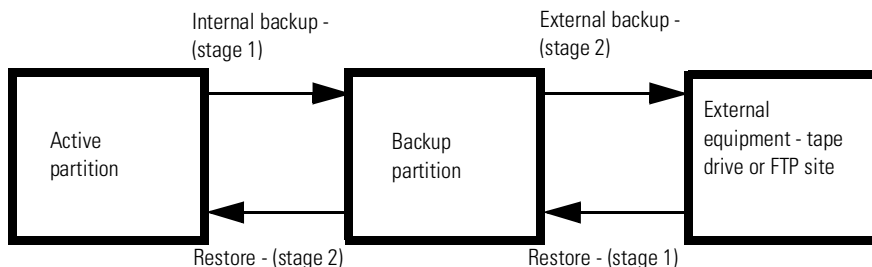
**Important:** When you successfully restore from a backup, Network Discovery assumes that all events are in an OK status for the first sampling period.

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 10-1: 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 131.

**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 If the option to choose tape is available, 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.
- ▶ 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 restore 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 restore 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.

Connect the cross over cable to Ethernet port 2 on the PND appliance.

**Figure 10-2: Ethernet port 2 on the IBM xSeries 335**

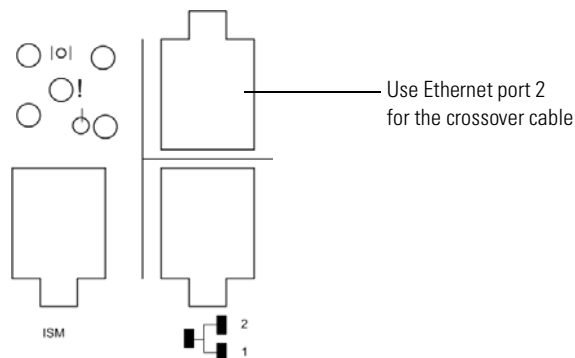
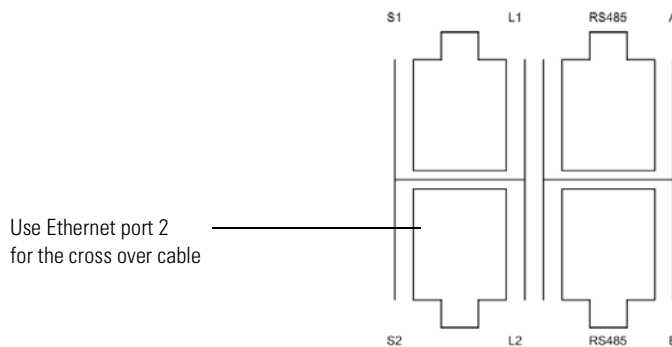


Figure 10-3: Ethernet port 2 on the IBM xSeries 330



#### 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 Select the backup file, then click **Restore**.
- 4 When the restore is complete, you can check the restore log by clicking **Administration > Backup and restore > View restore log**.



# 11

CHAPTER

## To Migrate from InfraTools Network Discovery or from Xanadu

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 migrate to PND 5.0.2 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
------------------------------	--

The hardware of the Peregrine appliance may be the same as the hardware of Xanadu 1.0.4. You can migrate Xanadu 1.0.4 to PND 5.0.2 by following the procedures in this chapter.

Topics in this chapter include:

- *How it works* on page 118
- *Upgrade the license on your new appliance* on page 120
- *Ensure that you have a backup from your old appliance* on page 120
- *Restore the old data to the new appliance* on page 121
- *You can keep your IND 4 style Seeds, Blocks and Forces* on page 122

## How it works

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

**Table 11-1: 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 9 Chapter 2, <i>Pre-setup Questionnaire</i> on page 13 Chapter 3, <i>Prepare the network</i> on page 21
Install the new appliance and start Network Discovery	Chapter 4, <i>Install and Start Network Discovery</i> on page 35
Log in to your new appliance	Chapter 5, <i>Appliance Management</i> , up to and including <i>Log in to Network Discovery</i> on page 50
Request and install your license on the new appliance	Chapter 6, <i>Licenses</i> on page 71
Take the backup from your old appliance and install it on the new one.	This chapter, <i>To Migrate from InfraTools Network Discovery or from Xanadu</i> and the previous chapter, Chapter 10, <i>Backup and Restore</i> on page 107.
Complete appliance management	Return to Chapter 5, <i>Appliance Management</i> , and carry on from and including <i>How to shut down the Peregrine appliance</i> on page 53 and so on...

The tasks for upgrading from Xanadu are almost the same, but, the order may be different. You can continue to use the IBM xSeries 330 server that Xanadu currently uses or you can choose to transfer to an IBM xSeries 335 server.

To upgrade with a transfer to the IBM xSeries 335 server, follow the order above in *What to do when you upgrade from IND*.

To upgrade Xanadu to PND 5.0.2, while keeping the same IBM xSeries 330 server that Xanadu currently uses, perform the tasks in the following order.



**Table 11-2: What to do when you upgrade from Xanadu (while keeping the same IBM xSeries 330 server)**

Task	Where to get information
Log in to your old appliance	Chapter 5, <i>Appliance Management</i> , up to and including <i>Log in to Network Discovery</i> on page 50
Take a backup from your old appliance	This chapter, <i>To Migrate from InfraTools Network Discovery or from Xanadu</i> and the previous chapter, Chapter 10, <i>Backup and Restore</i> on page 107.
Get started and prepare	Chapter 1, <i>Welcome to Network Discovery</i> on page 9 Chapter 2, <i>Pre-setup Questionnaire</i> on page 13 Chapter 3, <i>Prepare the network</i> on page 21
Install the new software and start Network Discovery	Chapter 4, <i>Install and Start Network Discovery</i> on page 35
Log in to your new appliance	Chapter 5, <i>Appliance Management</i> , up to and including <i>Log in to Network Discovery</i> on page 50
Request and install your license on the new appliance	Chapter 6, <i>Licenses</i> on page 71
Restore your old data to the PND 5.0.2 Peregrine appliance.	This chapter, <i>To Migrate from InfraTools Network Discovery or from Xanadu</i> and the previous chapter, Chapter 10, <i>Backup and Restore</i> on page 107.
Complete appliance management	Return to Chapter 5, <i>Appliance Management</i> , and carry on from and including <i>How to shut down the Peregrine appliance</i> on page 53 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

If you were using IND, 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 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.

To upgrade the license

- 1 Log in, following the instructions in *Log in to Network Discovery* on page 50.
- 2 Follow the instructions in Chapter 6, *Licenses* on page 71.

## Ensure that you have a backup from your old appliance

- ▶ Following the procedures in *Backup and Restore* on page 107, make sure that you have the backup you want to use.

**Note:** The backup for IND 4.2 or 4.3 must be from an internal backup or an external backup on an FTP server. The backup for Xanadu must be from an FTP server.

**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. The backup for Xanadu must be external.

**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

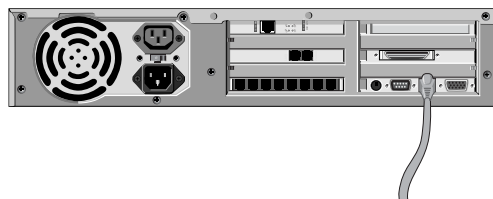
To restore the old data to the new appliance (IND to PND)

For Xanadu, go to step 2. (The backup for Xanadu must be from an FTP server.)

- 1 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.

**Figure 11-1: IND appliance cross over connection**



On the IBM xSeries server, connect to Ethernet port 2.

**Figure 11-2: Ethernet port 2 on the IBM xSeries 335**

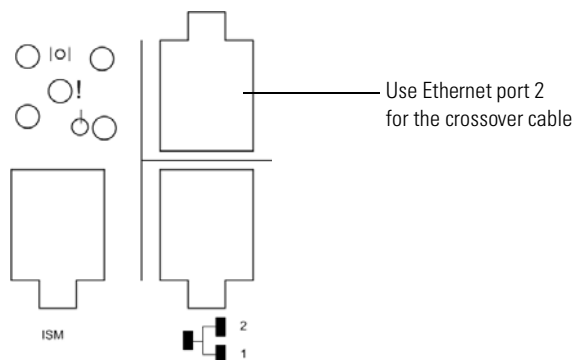
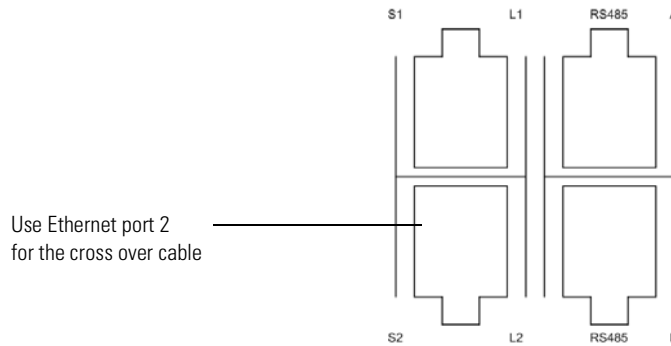


Figure 11-3: Ethernet port 2 on the IBM xSeries 330



- 2 Following the procedures in *Backup and Restore* on page 107, restore the backup you want to use.

Your software and licenses have been upgraded. You can now use PND 5.0.2. Continue with the procedures in Chapter 5 *Appliance Management* on page 49.

## You can keep your IND 4 style Seeds, Blocks and Forces

If you have upgraded from InfraTools Network Discovery 4.2. or 4.3 or Xanadu 1.0.4, 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 or Xanadu documentation.

# 12

## 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 124*
- *Check that your maintenance license is current on page 124*
- *Check that you have the latest software components on page 124*
- *Download the new component(s) on page 125*
- *Install the new component(s) on page 125*
- *After you install new components on page 125*

## 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 > Current Settings > Installed Licenses**
- 2 See the value of the attribute, “Maintenance valid until.”

## Check that you have the latest software components

Peregrine continually improves Network Discovery with new software components to handle new devices on the market and in your network.

**Note:** All downloadable components are cumulative; that is, the latest version includes all earlier improvements.

To check that you have the latest software components

- 1 Click **Status > Current settings > Installed components**
- 2 In particular, see the value of the attributes, “jay”, “rulebase”, and “servicepack”.

**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 component(s)

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

## 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 Administrator (or IT Manager) 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 > Current Settings > Installed components.**

If you installed jay or rulebase 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.

- 4 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 goes 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.

- Step 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.

Information about the firewall ports to enable is in *Choose how to receive Peregrine Systems Customer Support* on page 24 and *Enable firewall ports* on page 26.

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

This is a documented community string, known to:

- Administrator 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.

There is more information in *Change the Peregrine appliance community strings* on page 57.

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

- Create a new Administrator account for the Network Discovery Administrator.
- (optional) Create a new Demo account for training users.
- Log into the new Administrator 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.

There is information about accounts in Chapter 9, *Accounts* on page 99.

**Step 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 change the password for the “admin” account.

“password” is a documented account password, known to:

- anyone at your site with access to 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.

There is information about accounts in Chapter 9, *Accounts* on page 99 and there is information about event filters in the *Network Discovery User Guide*.

**Step 5** Change the Peregrine appliance’s default password (“Appliance”) in the configuration interface.

This is a documented password, known to:

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

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

There is information about how to change the Peregrine appliance's password in *Give the Peregrine appliance its network information* on page 39.



# 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.

## 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.

## Adding a CPU or a modem later

You can add a second Pentium III 1.4 GHz or better processor to an IBM xSeries 330 version of the Peregrine appliance to increase its capacity from a maximum of 5,000 to a maximum of 10,000 devices.

You can add an internal modem to either the IBM xSeries 335 or the IBM xSeries 330. An internal modem is used with an analog telephone line to give access to Peregrine Systems Customer Support.

When you add an internal modem or a second CPU after the initial software installation, you must use the Network Discovery installation CD to reboot the system.

## Use the CD and reboot the Peregrine appliance

Follow the manufacturer's instructions to add the CPU or modem. Then update your Network Discovery software.

To update the Network Discovery software, you need the following:

- A system server as specified in *Check the server that will be the Peregrine appliance* on page 28. All of the hardware components must be installed before the Network Discovery software is installed.
- A Network Discovery installation CD. The CD can be the currently installed version of Network Discovery or a later version. (Any software components that you have downloaded and installed are retained.)
- (Optional) A monitor and PS2 keyboard attached to the Peregrine appliance. (An alternative is to use the management workstation to restart the Peregrine appliance through the browser interface at **Administration > Appliance Management > Appliance Restart.**)

---

**Important:** A USB keyboard is not supported.

---

To update Network Discovery software:

- 1 Place the Network Discovery installation disc in the CD-ROM drive of the server and restart the server.

The system boots from the CD. During the reboot, the installation CD detects the new CPU or modem and ensures that the latest packages required for Network Discovery will be used. After the packages have been installed, the CD ejects, and the server reboots.

- 2 Remove the CD and store it in a safe place.

Network Discovery can now use the added CPU or modem.

If you see an error message telling you that there is a problem with the hardware, contact Peregrine Systems Customer Support.



# Index

---

## A

- AC power
  - connecting 36, 46
- account
  - change type 104
  - create a password 104
  - creating 102
  - pre-installed 100
  - setup 99
  - types
    - Administrator 100
    - Demo 100
    - IT Employee 100
    - IT Manager 100
- activate changes 80
- admin account *see* Administrator account
- Administrator account 100
  - password, changing 68
- alarms
  - turn off *see* disabling warnings 69

## B

- backup
  - FTP 109
  - immediate 112
    - external 112
    - internal 112
  - tape 109, 133
  - test 111
- backup warnings
  - enable/disable 70

- BIOS boot sequence 37
- block *see* IND 4 style configuration, keeping, *see also* network configuration, set up IPv4 ranges to avoid

## C

- CD
  - software installation 38
- Central Processing Unit *see* CPU
- changes, activating configuration changes 96
- CIR values 28
- Cisco devices 28
- collect information 13
- collecting information 11
- color settings 31
- Committed Information Rate values 28
- Community Property Groups 92
- community strings
  - about 23
  - changing Peregrine appliance 57
  - deleting 95
  - directed 23, 94
  - Global Community Property Group 79
  - multiple strings 94
  - SNMP traps 94
- components
  - see* software components
- configuration interface 36
- connecting power 36, 46
- copying map configurations 102
- CPU

adding later 133  
 Peregrine appliance specifications 29, 30

**D**

data backup 133  
 date and time  
   setting 65  
   synchronizing  
     continually 67  
     once 66  
 default map configuration 101  
 Demo account 100  
 device, disconnecting 101  
 DHCP 17, 22  
   static address for Peregrine appliance 14  
 DHCP servers 78  
 directed community strings 23, 94  
 disabling warnings 69–70  
   about 69  
 Domain Name Server, entering 59  
 domain search order, entering 59  
 Dynamic Host Configuration Protocol *see* DHCP

**E**

E-mail  
   Peregrine appliance administrator, changing  
     63  
 Exceptions reports 81  
 external modem 133

**F**

firewall ports 26–28  
   customer service access 25, 119  
 Frame Relay, set up 28

**H**

hardware  
   extra 131  
     CPU 133  
     external modem 133  
     internal modem 133  
     tape drive 133  
     UPS 131  
 hardware requirements 28  
 Home page 53

Host name, entering 61  
 Hot Standby Routing Protocol *see* HSRP  
 HSRP 22

**I**

installation  
   before you install the Peregrine appliance 9  
   checking the management workstation 31  
   hardware  
     CPU 133  
     external modem 133  
     extra 131  
     tape drive 133  
     UPS 131  
   preparing the network 21  
   software 38  
   software setup 49  
 Internet Explorer  
   minimum version 31  
   virtual machine 31  
 Internet firewall ports 119  
 IPv4 address 14, 39  
 IT Employee account 100  
 IT Manager account 100

**J**

Java  
   enable 31  
   environments 32  
 JavaScript  
   enable 31

**L**

license 71–73  
   default 72  
   install 73  
   maintenance 72  
   maintenance license  
     check if current 124  
   request 72  
 log on, initial 50

**M**

managed device  
   definition 14

- management console *see* management workstation 31
- management workstation requirements 31
  - browser 31
  - CPU 31
  - memory 31
  - video 31
- map configuration, default 101
- modem 133
  - external 133
  - internal
    - adding later 133
- modem warnings
  - enable/disable 70
- MTBF 101
- MTTR 101
- multiple community strings 94

**N**

- Netscape, minimum version 31
- network configuration 75–97
  - add DHCP servers 78
  - add IPv4 range 77
  - add IPv4 ranges 76, 77
  - add unmanaged routers 78
  - apply changes 96
  - community strings 79
  - delete IPv4 ranges 77
  - Property Groups 86
  - review and activate changes 80
  - reviewing and activating changes 96
  - set up IPv4 ranges to avoid 78
  - troubleshooting 80
- network discovery 75–97
- Network map session
  - disconnecting 101
- network preparation 13
- Network Property Group
  - apply to a range 92
  - create 90, 91
  - delete 91
  - modify 90, 91
- Network Property Groups 86–92
- node and subnode setup 14
- NTP server 67

**P**

- paging
  - external modem 133
- password
  - change Peregrine appliance default 41
  - changing for Administrator 68
  - create 104
- Peregrine appliance
  - no response after changing domain name server 61
  - shutdown 53
- Peregrine appliance administrator
  - e-mail address, changing 63
- Peregrine Appliance community strings
  - changing for security 57
- Peregrine appliance hardware requirements 28
- Peregrine Systems Customer Support
  - access options 24–28
    - Internet 25
    - Remote Access Server 26
    - telephone line 26
    - Virtual Private Network 25
  - firewall ports 119
- Peregrine Systems Customer Support access 15
- power
  - connecting 36, 46
- pre-installation 9
  - checking the management workstation 31
  - preparing the network 21
  - questionnaire 11, 13
- pre-installed accounts 100
- preparation 10
- preparing the network 21
- pre-setup 9
  - questionnaire 11
- Pre-setup Questionnaire 13
- Property Groups 86
- Property sets 96

**Q**

- questionnaire 13

**R**

- RAS 26
- Remote Access Server 26

- requirements
  - management workstation 31
  - Peregrine appliance 28
- resolution 31
- restore
  - another appliance 114
  - FTP backup 113
  - internal backup 113
  - tape backup 114
- restoring your data 113
- review and change configuration 96

**S**

- screen resolution 31
- security checklist 127
- Seeds, Block, Forces *see also* network configuration
- Seeds, Blocks, Forces *see* IND 4 style Seeds, Blocks, Forces 122
- server requirements 28
- setting the date and time 65
- setting the time zone 58
- setup 10
  - collecting network information 11
- setup, software 49
- shut down Peregrine appliance
  - browser interface 53
  - configuration interface 42
- SMTP Server, entering 63
- SNMP
  - traps 94
  - turn on
    - in network devices 23
    - in routers and switches 22
- SNMP management
  - definition 14
- software
  - installing 38
- software components 123–126
  - check if latest 124
- software setup 49
- software upgrades 123–126
- specifications
  - management workstation 31
  - Peregrine appliance 28
- synchronizing the date and time 66, 67

- system account 100

**T**

- tape drive 133
- telephone line 26
- time and date
  - setting 65
  - synchronizing
    - continually 67
    - once 66
- time zone, setting 58
- Toolbar, main 54
  - banner 55
  - buttons 55
  - status window 56
- traps, SNMP 94
- troubleshooting
  - at startup 80
  - Exceptions reports 81
  - when logging in 51

**U**

- unmanaged routers 78
- upgrading from IND 4.2 or 4.3 117–122
- upgrading from PND 5.0 *see the Network Discovery 5.0.1 Release Notes*
- upgrading from Xanadu 1.0.4 117–122
- upgrading software 123–126
- UPS 131
  - acceptable units 131
  - connecting 46
- UPS warning, enable/disable 69, 70

**V**

- virtual machine in Internet Explorer 31
- Virtual Private Network 25
- voltage switch 46



