

Peregrine

Network Discovery Setup Guide

Version 5.2.1

Copyright © 2004 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® and Network Discovery® are registered trademarks of Peregrine Systems, Inc. or its subsidiaries. Microsoft, Windows, Windows NT, Windows 2000, and other names of Microsoft products referenced herein are trademarks or registered trademarks of Microsoft Corporation. DB2 is a registered trademark of International Business Machines Corp.

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

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

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

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

This edition of the document applies to version 5.2.1 of the licensed program.

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



Contents

Chapter 1	Welcome to Network Discovery	9
	About Network Discovery	10
	Peregrine Desktop Inventory can contribute data to Network Discovery	10
	Why it's important to prepare	10
	Start by collecting information about your network	11
Chapter 2	Pre-setup Questionnaire	13
	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?	19
	Send the questionnaire	20
Chapter 3	Prepare the network	21
	Turn on SNMP management in all routers and core switches	22
	(Optional) Turn on SNMP management in other devices.	22
	Set DHCP lease time	23
	About community strings	23
	Give the Peregrine appliance IP address to all devices using directed community strings	24

	(Optional) Adjust bridge aging	24
	Plan the device and port to which the Peregrine appliance will be attached	25
	Choose how to receive Peregrine Systems Customer Support	26
	Through Internet access.	26
	Virtual Private Network over the Internet	27
	By modem and dedicated telephone line.	27
	Through a Remote Access Server (RAS)	27
	Enable firewall ports	28
	Check Cisco devices	31
	(Optional) Enable UDP port forwarding on routers	31
	Check Committed Information Rate (CIR) values	32
Chapter 4	Compatibility Matrix	33
	Picking the right Server	35
	Basic Requirements	35
	Small Appliance (up to 4,000 devices)	36
	Medium Appliance (up to 8,000 devices)	36
	Large Appliance (up to 15,000 devices)	37
	Servers that have been tested.	39
	Check the management workstation.	40
	Peregrine Product Compatibility	41
Chapter 5	Install and Start Network Discovery	43
	About installing the hardware	44
	Connect a keyboard and monitor directly to the Peregrine appliance	44
	Connect the Peregrine appliance to AC power	45
	Set the BIOS boot sequence	46
	IBM Hardware	46
	Dell Hardware.	48
	HP Hardware	51
	Install Network Discovery software from the CD	53
	Give the Peregrine appliance its network information	54
	Connect the appliance to the network	59
	Top-of-the-network device	59
	IBM xSeries 335 Peregrine appliance	59

	IBM xSeries 330 Peregrine appliance	60
	Dell 1750 Peregrine appliance	60
	Dell 1650/2650 Peregrine appliance	61
	HP DL360/DL380 Peregrine appliance	61
	Connect a management workstation to the network	62
	Connect an Uninterruptible Power Supply	63
	(Optional) Connect data backup equipment and pager hardware	64
	(Optional) Connect the Peregrine appliance to a telephone line	65
	(Optional) Using terminal emulation software	66
Chapter 6	Appliance Management	67
	Log in to Network Discovery	68
	Troubleshooting when logging in for the first time	69
	The Home page	72
	The Toolbar	73
	The banner or title bar	73
	The status window	73
	Assign a system name, contact, and location	74
	Change the Peregrine appliance community strings	75
	Set the time zone	76
	Enter the domain name server	77
	Enter the host name	79
	(Optional) Enter the Workgroup name	80
	(Optional) Enter the Administrator e-mail address	81
	(Optional) Enter the SMTP server	82
	Set the system time	83
	Set the date and time	83
	Synchronize the time	84
	Enter an NTP server to synchronize the time (continually)	85
	Change the default Admin password	86
	About disabling warnings	87
	Disabling UPS warnings	88
	Disabling modem warnings	88
	Disabling backup warnings	89

Chapter 7	Licenses	91
	How it works	92
	Request a new license	93
	Install the new license.	94
Chapter 8	Set up Network Discovery	95
	How it works	96
	Run router discovery	97
	Set up the IPv4 range(s) to discover	98
	Import your IPv4 ranges from a CSV file	98
	View an IPv4 range.	99
	Export your IPv4 ranges to a CSV file	99
	Delete an IPv4 range	100
	Add an IPv4 range	100
	Set up the IPv4 range(s) to avoid	101
	Add ranges for DHCP servers and unmanaged routers	102
	Add community strings—the quick way	103
	Activate your proposed changes	104
	Check that it's working	105
	Are devices appearing on the Network Map?	105
	Are there problems on the Exceptions reports?	105
	Check the Device Filters report.	106
	Check the Device Modeling Queue	106
Chapter 9	Refining Network Discovery	107
	A precise matrix of network discovery	108
	A tree of IPv4 ranges	108
	Property Groups	110
	Network Property Groups	111
	The properties.	112
	How to use Network Property Groups.	114
	Making changes to Network Property Groups	115
	Modify a Network Property Group	115
	Create a Network Property Group	116
	Delete a Network Property Group	116

	Apply a Network Property Group to a range	117
	Community Property Groups	117
	More on community strings	119
	Multiple Strings	119
	SNMP Traps	120
	Directed Community Strings	120
	Deleting a community string.	121
	Property sets are a shortcut	122
	Reviewing and activating your configuration changes	123
Chapter 10	Setting up Accounts	125
	There are four pre-installed accounts	126
	How many people can use Network Discovery at once	126
	How the types of accounts differ	127
	Creating accounts	127
	(Optional) More Account Administration	130
Chapter 11	Backup and Restore	131
	About external backups	132
	Choosing tape or an FTP site for your external backup	133
	Configuring an external backup	134
	Testing your external backup and restore	136
	To run an internal or external backup immediately	138
	Restoring your data.	139
	Restoring from the internal backup	139
	Restoring from an FTP site	140
	Restoring from tape	140
	Restoring from another appliance	141
Chapter 12	Shutting down the Peregrine Appliance	145
	How to shut down the Peregrine appliance	145
Appendix A	Before you call...	147
	Overview	148
	Check that your maintenance license is current	148
	Check that you have the latest software components	148

	Download the new component(s).	149
	Install the new component(s)	149
	After you install new components.	150
Appendix B	Security Checklist.	151
Appendix C	Extra Hardware	155
	Uninterruptible Power Supply (UPS) units.	155
	Acceptable UPS units.	156
	Recommended UPS units for Africa, Asia, Europe, Australia, the Middle East, and the South Pacific.	156
	Recommended UPS units for North America.	156
	Tape Drive	157
	External Modem	157
	Adding a CPU or a modem later	158
	Use the CD and reboot the Peregrine appliance.	158
	Index.	161

1 Welcome to Network Discovery

CHAPTER

Thank you for using 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 is critical to your success with Network Discovery. Your sales representative may have given it to you as a separate pre-purchase handout (*Preparing for Installation*); or you may be seeing it for the first time as the first four 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 5, *Install and Start Network Discovery*. If you are seeing this information for the first time, let's get started.

Important: Instructions for upgrading from Network Discovery 5.0, 5.0.1, 5.0.2, 5.1, 5.1.1, 5.1.2, or 5.2 are in the 5.2.1 *Release Notes*.

About Network Discovery

Network Discovery is a real-time web-based network manager. When integrated into your network, Network Discovery will discover and monitor all devices in your network. You will use Network Discovery to find, diagnose and solve network problems.

Peregrine Desktop Inventory can contribute data to Network Discovery

Peregrine Desktop Inventory (PDI) scanners can be scheduled from Network Discovery and scan files can be added to a shared directory on the Peregrine appliance, so the scanned devices will appear in the Network Discovery database, and on the Network Map.

For more information on setting up PDI to contribute data to Network Discovery, see *Using Network Discovery with Desktop Inventory and Desktop Administration*.

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 Pre-Setup Questionnaire is available in the next chapter of this manual (see *Pre-setup Questionnaire* on page 13), from your sales representative, or as a Word file from <http://support.peregrine.com>.

Note: If you wish, you may fill in the questionnaire and send it to Peregrine customer support. They can review your information and provide feedback on how you set up Network Discovery.

If you have already filled out this form and sent it in to Peregrine customer support, collecting all the information is done. Keep the completed questionnaire handy.

The questionnaire is designed to make the setup and use of 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 customer support offices are available through Peregrine's CenterPoint Web site at <http://support.peregrine.com>.

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 26.

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		

	From	To
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 the DHCP server ARP cache 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?

Warning: Do not mirror your hard drives, and do not install RAID in your Peregrine appliance. If you do, your appliance will not function properly.

Please check one (for more information, see *Compatibility Matrix* on page 33):

IBM xSeries 335

Small - 2GB, 1 CPU _____

Large - 4GB, 2 CPUs _____

IBM xSeries 330

Small - 1GB, 1 CPU _____

Medium - 2GB, 2 CPUs _____

Dell 1750 Servers

Small - 2GB, 1 CPU _____

Large - 4GB, 2 CPUs _____

Dell 1650 Servers

Small - 1GB, 1 CPU _____

Medium - 2GB, 2 CPUs _____

Dell 2650 Servers

Large - 4GB, 2 CPUs _____

HP DL360

Large - 4GB, 2 CPUs _____

HP DL380

Large - 4GB, 2 CPUs _____

Note: Any of the “Large” appliances can be turned into a “Medium” appliance by removing 1 CPU and 2 GB of RAM.

Send the questionnaire

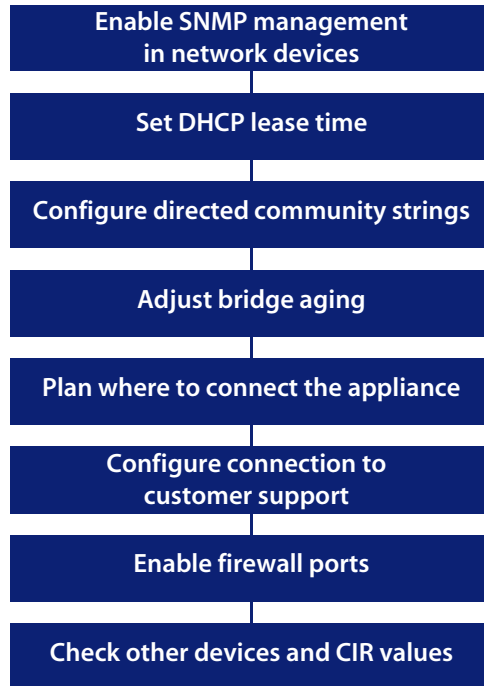
When you have completed the questionnaire, send it to Peregrine Systems Inc. by e-mail, mail or by fax. To find the mailing address or fax number of the Peregrine office in your region, contact your OEM/VAR or check <http://support.peregrine.com>.

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

3 Prepare the network

CHAPTER

The following flowchart shows all the important tasks that must be completed to prepare your network. There are other optional tasks described throughout the chapter.



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.

(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.

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.

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 (ottongw.peregrine.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	
Applet Server	8109/tcp	

Note:

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 5, *Install and Start Network Discovery* on page 43.

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
Echo Reply	0/icmp		device	Peregrine appliance
Error Messages	3/icmp		device	Peregrine appliance
Echo Request	8/icmp		Peregrine appliance	device
TTL Timeout	11/icmp	5	Peregrine appliance	device
			device	Peregrine appliance
Netmask Request	17/icmp		Peregrine appliance	device
Netmask Reply	18/icmp		device	Peregrine appliance
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

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

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
Peregrine Listener	1738/udp	4	Peregrine appliance	device with Peregrine Desktop Inventory (PDI) Listener
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
Applet server	8109/tcp		management workstation	Peregrine appliance
		2	Peregrine appliance	aggregated Peregrine appliance
ServiceCenter	12670/tcp	6	Peregrine appliance	ServiceCenter server

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

Traceroute	33263/udp 33436/udp	Peregrine appliance	device
------------	------------------------	---------------------	--------

Note:

1. Depending on your settings for Appliance proxy services
2. If you have and Aggregator license
3. If you are using SNMP trap notification
4. This listener port is the default. You can add more ports for Network Discovery to listen on in **Administration > System preferences > Listener communication**
5. TTL Timeout can go in either direction, from the Peregrine appliance or to the Peregrine appliance.
6. You can change this port at **Administration > System preferences > ServiceCenter configuration**.

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.

(Optional) Enable UDP port forwarding on routers

If you want to have your Peregrine appliance communicate with listener agents across subnets, you will need to enable routing for the UDP packets. If you have routers separating the broadcast domains in your network, you should configure them to pass along listener broadcast traffic on port 1738, as well as on the ports you have configured on your Peregrine appliance.

Note: Port 1738 is the default, but you can add other listener ports in **Administration > System Preferences > Listener communication**.

By configuring the Peregrine appliance and your routers to listen for UDP broadcasts on the same ports, Network Discovery will find new workstations much faster.

For Cisco routers, a procedure is provided below. For any other manufacturer, Peregrine recommends checking the router documentation to find a way to forward UDP traffic between subnets.

To configure your Cisco IOS router

- 1 Access the EXEC privilege level on the configuration interface.
- 2 Enter the following commands:

```
configure terminal <enter>
interface [source interface] <enter>
ip helper-address [destination listener] <enter> (repeat this command for
each appliance you want to send to)
exit <enter>
ip forward protocol udp 1738 <enter>
end <enter>
```

Note: Any interface can have multiple helper-addresses.

Note: The “ip forward protocol upd” command specifies the ports to forward. In this case, we recommend port 1738. You will need to list other ports if you have configured other listener ports in **Administration > System Preferences > Listener communication**.

- 3 Exit the configuration interface.

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.

4 Compatibility Matrix

CHAPTER

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

For a new installation, the IBM xSeries 335, Dell 1750 Server, or HP DL360/DL380 are recommended. However, the IBM xSeries 330 or Dell 1650 can also be used. More specific hardware information is available later in this chapter.

Warning: Do not mirror your hard drives, and do not install RAID in your Peregrine appliance. If you do, your appliance will not function properly.

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

Note: There is no need to order a keyboard, mouse, operating system, or monitor; you can use existing hardware you have on hand.

The following table should help you decide what size of appliance(s) you will need.

Table 4-1: Recommended values for each appliance size

	Small Appliance 1 CPU, 1GB RAM	Medium Appliance 2 CPUs ^a , 2GB RAM	Large Appliance 2 CPUs ^b , 4GB RAM
Regular Appliance			
Devices	4,000	8,000	15,000
Ports	24,000	48,000	90,000
Attributes	560,000	1,120,000	2,100,000
Aggregator Appliance			
Devices	20,000	50,000	100,000
Ports	120,000	300,000	600,000
Attributes	2,800,000	7,000,000	14,000,000
Appliances	10	20	50

a This could be 2 CPUs, or one physical CPU which is equivalent to 2 logical CPUs.

b The large appliance has 2 physical CPUs, which is equivalent to 4 logical CPUs.

However, if you are using your Peregrine appliance in Basic Discovery mode, the number of devices (scan files) change considerably. For more information on Basic Discovery licenses, see *Basic Discovery License* on page 92.

	Small Appliance 1 CPU, 1GB RAM	Medium Appliance^a 2 CPUs, 2GB RAM	Large Appliance 2 CPUs, 4GB RAM
Devices	25,000	30,000	100,000
Ports	150,000	180,000	600,000
Attributes	25,000	30,000	100,000

a In order to support 40,000 devices on the Medium appliance, you must have 73GB disks.

Important: If you are using the Desktop Inventory delta scanning feature, the amount of disk space required for scan files doubles because both the enriched scan and the original scan are kept. On appliances where disk space may be fully used, the number of devices to be managed may need to be reduced by half. For example, a large appliance may only be able to support 30,000 devices. Peregrine estimates that an average scan file would be 270 KB.

Picking the right Server

Each appliance recommended here is known to work with the Network Discovery software. If you have another appliance you want to use, contact customer support to see if that appliance has been tested since this manual was printed.

Note: The appliance you select will depend on the size of your network.

Basic Requirements

The Network Discovery software should work if the hardware meets the minimum requirements:

- 1 CPU, 2.4 GHz or better, with 512KB full-speed cache
- at least 1GB of RAM (or more depending on the number of devices)
- 2 SCSI drives with a minimum of 36 GB each
- Dell, HP, or IBM server

Warning: Peregrine cannot guarantee that all devices with these requirements will work. For best results, choose one of the tested platforms.

Small Appliance (up to 4,000 devices)

IBM

IBM xSeries 335 with:

- 1 CPU
- 1GB RAM
- 2 x 36 or 73GB SCSI disks

IBM xSeries 330 with:

- 1 CPU
- 1GB RAM
- 2 x 36 or 73GB SCSI disks

Dell

Dell 1650 Server with:

- 1 1.26Ghz CPU
- 1GB RAM
- 2 x 36GB or 73GB 10,000 RPM SCSI disks

Dell 1650 Server with:

- 1 1.40Ghz CPU
- 1 GB RAM
- 2 x 36GB or 73GB 10,000 RPM SCSI disks

Medium Appliance (up to 8,000 devices)

IBM

IBM xSeries 335 with:

- 1 CPU
- 2GB RAM
- 2 x 36GB or 73GB SCSI disks

IBM xSeries 330 with:

- 2 CPUs

- 2GB RAM
- 2 x 36GB or 73GB SCSI disks

Dell

Dell 1750 Server with:

- 1 x 2.40Ghz XEON CPU
- 2 (or more) GB RAM
- 2 x 36GB or 73GB 10,000 RPM SCSI disks

Dell 1750 Server with:

- 1 x 3.0Ghz XEON CPU
- 2 (or more) GB RAM
- 2 x 36GB or 73GB 10,000 RPM SCSI disks

Dell 1750 Server with:

- 1 x 2.40Ghz/533MHz Bus XEON CPU
- 2 (or more) GB RAM
- 2 x 36GB or 73GB 10,000 RPM SCSI disks

Dell 1750 Server with:

- 1 x 2.80Ghz/533MHz Bus XEON CPU
- 2 (or more) GB RAM
- 2 x 36GB or 73GB 10,000 RPM SCSI disks

Dell 1750 Server with:

- 1 x 3.06Ghz/533MHz Bus XEON CPU
- 2 (or more) GB RAM
- 2 x 36GB or 73GB 10,000 RPM SCSI disks

Large Appliance (up to 15,000 devices)

IBM

IBM xSeries 335 with:

- 2 CPU

- 4GB RAM
- two 73GB SCSI disks

Dell

Dell 1750 Server with:

- 2 x 2.40, 2.80, or 3Ghz XEON CPU
- 4 GB RAM
- 2 x 36GB or 73GB 10,000 RPM SCSI disks

Dell 2650 Server with:

- 2 x 2.00 Ghz XEON CPU
- 4 GB RAM
- 2 x 73GB SCSI disks

HP

HP DL360/DL380 with:

- 2 x Intel® Xeon 3.06 GHz CPU (1 MB L2 cache)
- 2 x 2 GB RAM (PC2100 DDR kit)
- 2 x 72.8GB disks (U320 universal SCSI 10,000 rpm)

Note: The disks must be installed in bays 0 and 1.

Servers that have been tested

Here is a list of servers that Peregrine has tested and do work:

Dell	<ul style="list-style-type: none">■ 1650■ 1750■ 2650
IBM	<hr/> <ul style="list-style-type: none">IBM 335■ 8676-11x■ 8676-21x■ 8676-61x■ 8676-81x■ 8676-J1XIBM 330■ 8674-41x <hr/>
HP	<ul style="list-style-type: none">HP DL360■ 337054-001HP DL380■ 293765-001 <hr/>

Check the management workstation

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

Table 4-2: Requirements and recommendations for the management workstation

Item	Required	Recommended
Web browser	Netscape 6.2.2 or later	Netscape 6.2.2 or later
	Internet Explorer 5.5 or later ^a	Internet Explorer 5.5 or later
	Mozilla 1.4 or later	Mozilla 1.6
Java Runtime Engine	1.4.1_01 or later ^b	1.4.1_01 or later (on Linux, 1.4.2 or later)
Video	16,000	65,000 or more
	—colors	
—resolution	800×600	1024×768 or more
Memory (MB RAM)	128 (512, if using an Aggregator)	512 ^c or more
CPU	Pentium II 233 equivalent or better	Pentium III 800 equivalent or better
Operating system		Windows 2000 or better
Microsoft Office		Microsoft Office 2003 (for processing csv export files)

a Requires a Virtual Machine (VM) upgrade.

b Must be downloaded from java.sun.com, do not use the version that comes with your browser

c 512 MB is recommended for large network maps.

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

Peregrine Product Compatibility

Table 4-3: Peregrine Products

Product	Compatible Version
ServiceCenter	5.1 or later
AssetCenter	4.3.1 or later
Connect-It	3.3.2 or later ^a
Desktop Inventory	7.3.0, 7.3.1, or 8.0 ^b

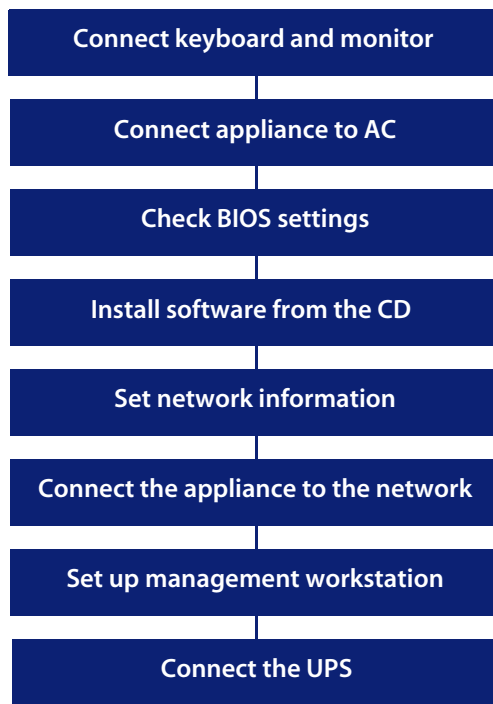
a Connect-It 3.3.2 supports UTF-8. The latest Connect-It scenario is included with version 3.3.2.

b You can set Network Discovery to work with scanners from Desktop Inventory 7.3.1 or 8.0. See **Administration > System preferences > Scanner Version**.

5 Install and Start Network Discovery

CHAPTER

The following flowchart shows all the important tasks that must be completed to install the appliance. There are other optional tasks described throughout the chapter.



About installing the hardware

When you install the server, follow the server installation documentation. The server installation documentation may vary depending on what 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.

Warning: Do not mirror your hard drives, and do not install RAID in your Peregrine appliance. If you do, your appliance will not function properly.

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.

Connect the Peregrine appliance to AC power

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

Set the BIOS boot sequence

IBM Hardware

You must configure the BIOS of the Peregrine appliance 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
USB Legacy	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.

Wake On LAN	Disabled
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.

Dell Hardware

You must configure the BIOS of the Peregrine appliance to use the correct boot sequence.

Note: The Dell 1750 and 1650 require some changes. The Dell 2650 will work properly with the default settings.

For the Dell 1750

To set the BIOS boot sequence

In the setup, use the up and down keys to select the items and the right and left keys to configure the options.

After you power the server on, wait until the display shows **Press F2 for Configuration/Setup**.

- 1 Press **F2**.
You see the Main menu.
- 2 In the main menu, make sure the Item “OS Install Mode” is set to “Off.”
- 3 Use the arrow keys to select **CPU Information** and press **Enter**.
- 4 Press **Enter** again.
- 5 Verify that the options are set as follows. Do not change options that are not listed here. Use the arrow keys to make changes.

Logical Processor	Enabled
Sequential Memory Access	Disabled

- 6 Press **Esc**.
You see the Main menu again.
- 7 Use the arrow keys to select **Boot Sequence** and press **Enter**.
- 8 Press **Enter** again.
- 9 Verify that the options are set as follows. Do not change options that are not listed here. Use the arrow keys to make changes.
 1. CD-ROM Device
 2. Hard Drive C:
 3. Embedded Primary MBA v6.2.6 Slot 0200
 4. Diskette Drive A:
- 10 Press **Esc**.

You see the Main menu again.

- 11 Use the arrow keys to select **Hard-Disk Drive Sequence** and press **Enter**.
- 12 Verify that the options are set as follows. Do not change options that are not listed here. Use the arrow keys to make changes.

1. Embedded #428 10X0,A:00
2. System BIOS boot devices

- 13 Press **Esc**.

You see the Main menu again.

- 14 Use the arrow keys to select **Integrated Devices** and press **Enter**.
- 15 Verify that the options are set as follows. Do not change options that are not listed here. Use the arrow keys to make changes.

Embedded SCSI Controller	SCSI
IDE CD-ROM Controller	Auto
Diskette Controller	Auto
USB Controller	On without BIOS support
Embedded GB NIC 1 + 2	On
NIC 1 PXE	Disabled
NIC 1 PXE	Disabled
Serial Port 1	COM1

- 16 Press **Esc**.

You see the Main menu again.

- 17 Use the arrow keys to select **Console Redirection** and press **Enter**.
- 18 Verify that the options are set as follows. Do not change options that are not listed here. Use the arrow keys to make changes.

Console Redirection	Off
---------------------	-----

Note: All other BIOS settings do not affect Network Discovery and can be set as you prefer (including asset tags, keyboard and security preferences, etc.).

For the Dell 1650

To set the BIOS boot sequence

In the setup, use the up and down keys to select the items and the right and left keys to configure the options.

After you power the server on, wait until the display shows **Press F2 for Configuration/Setup**.

- 1 Press **F2**.
You see the Main menu.
- 2 In the main menu, make sure the Item “OS Install Mode” is set to “Off.”
- 3 Use the arrow keys to select **Boot Sequence** and press **Enter**.
- 4 Press **Enter** again.
- 5 Verify that the options are set as follows. Do not change options that are not listed here. Use the arrow keys to make changes.
 1. CD-ROM Device
 2. Hard Drive C:
 3. Diskette Drive A:
- 6 Press **Esc**.
You see the Main menu again.
- 7 Use the arrow keys to select **Hard-Disk Drive Sequence** and press **Enter**.
- 8 Verify that the options are set as follows. Do not change options that are not listed here. Use the arrow keys to make changes.
 1. AIC-7899, A:00
 2. System BIOS boot devices
- 9 Press **Esc**.
You see the Main menu again.
- 10 Use the arrow keys to select **Integrated Devices** and press **Enter**.
- 11 Verify that the options are set as follows. Do not change options that are not listed here. Use the arrow keys to make changes.

Embedded SCSI Controller	SCSI
IDE CD-ROM Controller	Auto
Diskette Controller	Auto
USB Controller	On without BIOS support

Embedded 1GB NIC 1	Enabled without PXE
Embedded 1GB NIC 2	Enabled without PXE
Serial Port 1	COM1

- 12 Press **Esc**.
You see the Main menu again.
- 13 Use the arrow keys to select **Console Redirection** and press **Enter**.
- 14 Verify that the options are set as follows. Do not change options that are not listed here. Use the arrow keys to make changes.

Console Redirection	Off
---------------------	-----

Note: All other BIOS settings do not affect Network Discovery and can be set as you prefer (including asset tags, keyboard and security preferences, etc.).

HP Hardware

For the HP DL360/DL380, you need to change its default Hard Drive settings, and the OS selection. By default, the server might be configured to see its two drives as one large logical drive. For Network Discovery to function properly, you need to reconfigure the options, so your server will appear to have two logical drives.

To configure the logical drives

After you power the server on, wait until the display shows **Press F8 for ROM Configuration Options**.

- 1 Press **F8**.
- 2 Use the arrow keys to go to **Delete Logical Drive** and press **Enter**.
- 3 Press **F8** to delete the logical drive.
A warning screen appears.
- 4 Press **F3** to confirm the delete.
A progress message appears that says “Saving Configuration.”
- 5 When the configuration is saved, press **Esc** to return to the main menu.
- 6 Use the arrow keys to go to **Create Logical Drive**.
- 7 Under **Available Physical Drives**, select only one.
- 8 Under **RAID Configuration**, select **RAID 0**.

- 9 Press **Enter**.
A confirmation message appears.
- 10 Press **F8** to confirm.
A progress message appears that says “Saving Configuration.”
- 11 When the configuration is saved, press **Esc** to return to the main menu.
- 12 Repeat step 6 to step 11 to create the second logical drive.
- 13 When both logical drives are configured, return to the main menu.
- 14 Use the arrow keys to go to **View Logical Drives**, and confirm that both drives have been configured properly.
- 15 Press **Esc** to return to the main menu.

To configure the correct OS

- 1 From the main menu, press **F10** to access the **System Maintenance Menu**.
- 2 Use the arrow keys to go to the **Setup Utility**.
- 3 Select **System options**.
- 4 Select **OS Selection** and press **Enter**.
- 5 Select **Linux** and press **Enter**.
- 6 Press **Esc** to exit.
- 7 Press **F10** to confirm the exit.

Install Network Discovery software from the CD

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

To install Network Discovery

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

Note: Network Discovery will install if you have 1, 1.5, 2, 2.5, or 4GB of memory. If you have more than 4GB, the software will not install. You must have the exact hardware configuration as described in *Compatibility Matrix* on page 33.

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 be reachable 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

1 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

1 Type 3 and press **Enter**.

2 Type the IP address of the Peregrine appliance.

3 Press **Enter**.

4 Type 4 and press **Enter**.

5 Type the netmask of the Peregrine appliance.

6 Press **Enter**.

7 Type 5 and press **Enter**.

8 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.

9 Press **Enter**.

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

10 Type 6 and press **Enter**.

11 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

1 Type 10 and press Enter.

2 Follow the screen prompts.

3 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 44.

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 from floppy
- 7) Copy listener security keys to floppy
- 8) Copy listener security keys from floppy

- 9) Check CD
- 10) Restore from internal backup
- 11) Create temporary account to reset administrator password

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 appliance 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.

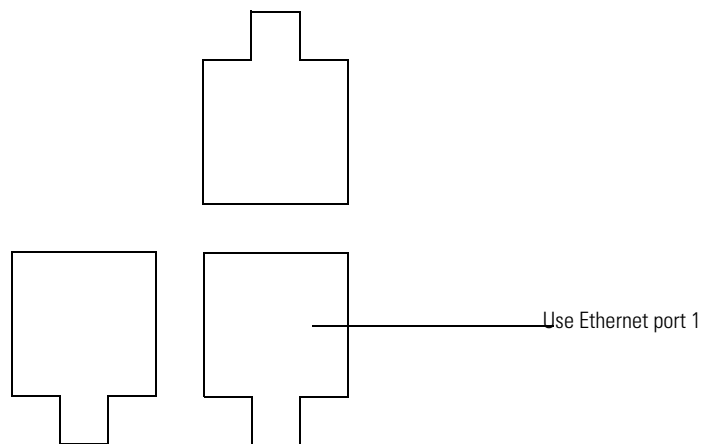
The port that allows the Peregrine appliance access to the network must be Ethernet. Network Discovery automatically detects what speed the Ethernet port is and whether it is full- or half-duplex. Network Discovery works best if the port is SNMP managed.

Note: Network Discovery's network interface card is configured to "auto negotiate." Make sure the switch to which you are connecting has its interface set to "auto negotiate."

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.

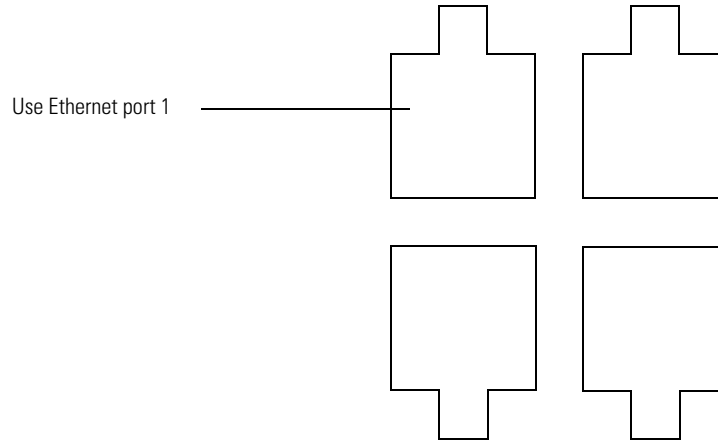
Figure 5-1: IBM xSeries 335 ports



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.

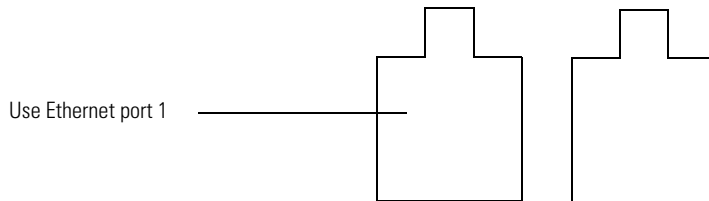
Figure 5-2: IBM xSeries 330 ports



Dell 1750 Peregrine appliance

On the Dell 1750 Server, connect the top-of-the-network device to the Peregrine appliance's Ethernet port 1, the left port.

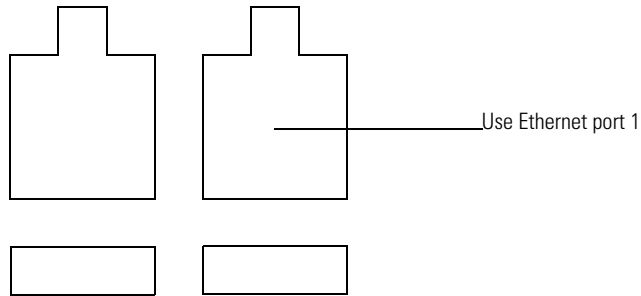
Figure 5-3: Dell 1750 Ethernet ports



Dell 1650/2650 Peregrine appliance

On the Dell 1650 or 2650 Server, connect the top-of-the-network device to the Peregrine appliance's Ethernet port 1, the right port.

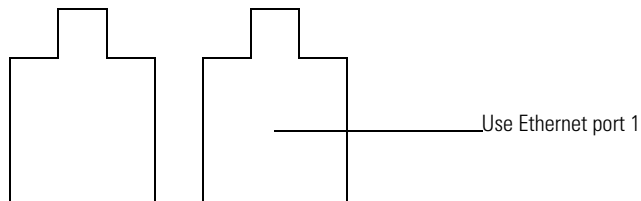
Figure 5-4: Dell 1650/2650 Ethernet ports



HP DL360/DL380 Peregrine appliance

On the HP Server, connect the top-of-the-network device to the Peregrine appliance's Ethernet port 1, the right port.

Figure 5-5: HP DL360/DL380 Ethernet 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

Connecting an uninterruptible power supply (UPS) is optional, but highly recommended. For information about UPS units that will work with the Peregrine appliance, see *Appendix C, Extra Hardware* on page 155.

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

Note: To suppress this warning, you need to turn off the “UPS warning,” see *Disabling UPS warnings* on page 88.

(Optional) 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 131.

For tape drive requirements, see *Appendix C, Extra Hardware* on page 155.

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 may 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 Peregrine appliance 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 26).

Note: If you decide to perform this procedure, you must have purchased an internal modem according to the specifications in *Compatibility Matrix* on page 33.

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.

Note: If you do not connect the Peregrine appliance to a telephone line, you will see a warning on the Appliance Health report (**Status > Appliance Health**). To suppress this warning, you need to turn off the “Modem Warning,” see *Disabling modem warnings* on page 88.

(Optional) Using 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 46).

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.

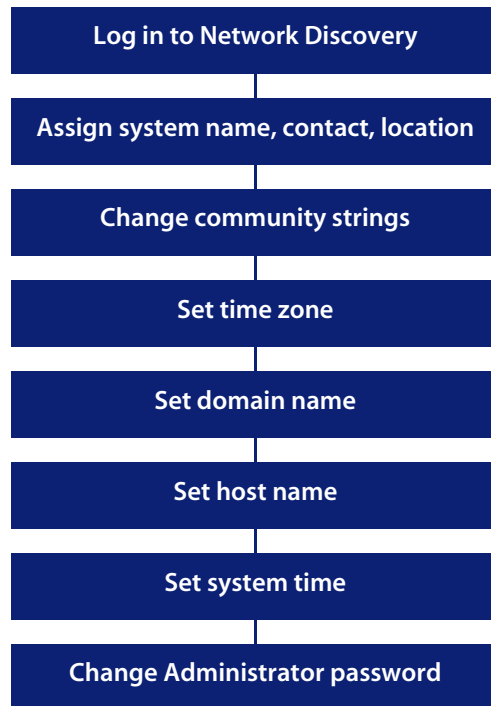
Table 5-1: Terminal requirements or settings

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

6 Appliance Management

CHAPTER

The following flowchart shows all the important tasks that must be completed to set up your appliance. There are other optional tasks described throughout the chapter.



Log in to Network Discovery

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

- access to a web browser with
 - Sun Java 1.4.1_01 or later enabled
 - Javascript enabled
 - pop-up windows enabled
- 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 6-1: 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, your browser will display one or more security warnings. You are asked to grant Network Discovery permission to run.
- 4 Click the check box next to “Always trust content from Peregrine Systems, Inc.” and click Yes.

Note: The security warning will differ depending on the browser you are using.

Note: This should be the only time you use the default password for the “admin” account. See *Change the default Admin password* on page 86.

Troubleshooting when logging in for the first time

Why can't I connect to Network Discovery?

- Check that you connected the Ethernet cable to the correct Ethernet port (see *Connect the appliance to the network* on page 59)
- 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.
- 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 54). 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.
- 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.

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, **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.

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. Three 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 6-1: Home page

The screenshot shows the 'Peregrine Network Discovery Home' page. On the left, there are two columns of navigation links with descriptions:

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

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

On the right, the 'Network Availability' section contains three line graphs showing network availability over time:

- Last 7 days**: A graph showing a steady state of high availability (near 100%) with a single dip on a Monday.
- Last 30 days**: A graph showing consistent high availability with several small dips.
- Last 90 days**: A graph showing a significant period of low availability (around 80%) in January and February, followed by a recovery to high availability in March.

At the bottom, a breadcrumb trail reads: [Home](#) | [Health Panel](#) | [Alarms Viewer](#) | [Network Map](#) | [Service Analyzer](#) | [Events Browser](#) | [MIB Browser](#) | [Find](#) | [Home](#) | [Reports](#) | [Administration](#) | [Status](#) | [Download](#) | [Help](#). The Peregrine logo is in the bottom right corner.

Links to major features

First row of hyperlinks shows where you have been

Bottom rows are is Toolbar buttons

The Network Availability graphs give you an idea of how your network is performing. In this example, you can see the appliance has been running for approximately 1.5 months.

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

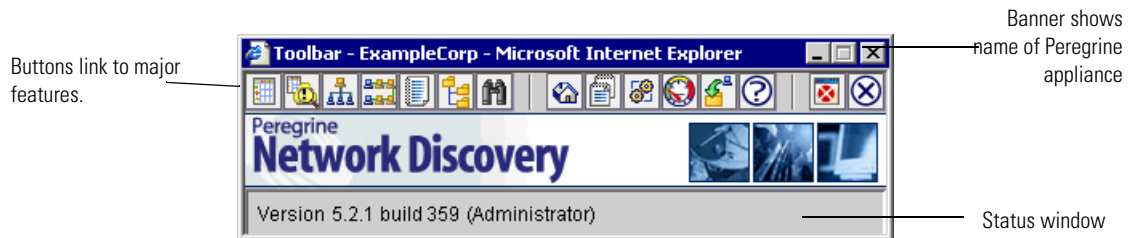
The Toolbar

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

- banner or title bar
- buttons
- status window

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

Figure 6-2: 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 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.

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.

Tip: If you wish, you can leave the write community string blank.

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

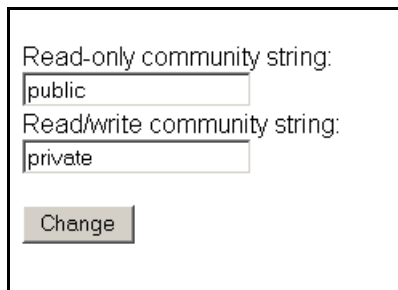
There is more information on community strings in:

- *About community strings* on page 23
- *Add community strings—the quick way* on page 103
- *More on community strings* on page 119

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 6-3: Change community strings



The screenshot shows a configuration window with two text input fields and a button. The first field is labeled "Read-only community string:" and contains the text "public". The second field is labeled "Read/write community string:" and contains the text "private". Below the fields is a button labeled "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.

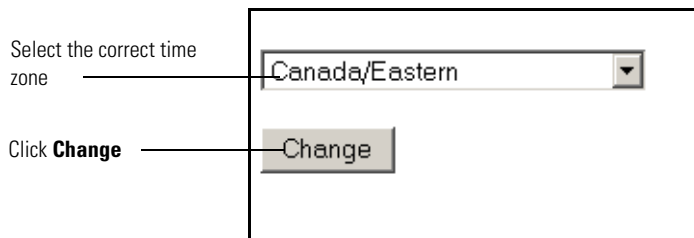
Warning: The time zone must be set when the Peregrine appliance is first set up. If the time zone has not been set, or if you change the time zone, the Network Map may not be updated for a period equal to the difference between the two time zones.

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 20 to 30 minutes.)

Figure 6-4: 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 names 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 either 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 “Find” 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 6-5: 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):
192.168.133.1,192.168.1.1

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

Change

Enter the host name

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

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

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

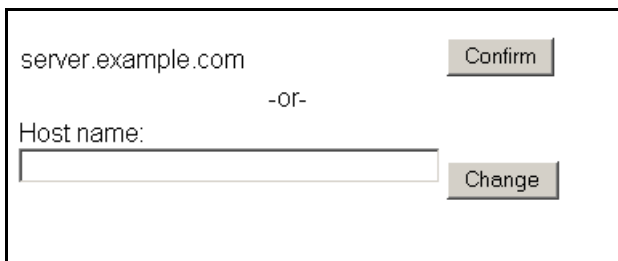
In prompted mode, Network Discovery will try to read its own host name from the domain name server. If Network Discovery finds a host name matching its IP address, you will be asked to confirm that the match is correct.

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

To change the host name

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

Figure 6-6: Change host name



The screenshot shows a web interface for changing the host name. At the top, the current host name "server.example.com" is displayed next to a "Confirm" button. Below this, the text "-or-" is centered. Underneath, the label "Host name:" is followed by an empty text input field and a "Change" button.

(Optional) 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 receive them from Peregrine Customer Support
- updated software components
- scan files

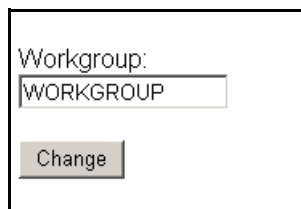
The current workgroup name is shown below. The default name is WORKGROUP.

The workgroup name must be 1-15 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**.

Figure 6-7: Change Workgroup



The screenshot shows a dialog box with a label 'Workgroup:' and a text input field containing 'WORKGROUP'. Below the input field is a 'Change' button.

(Optional) 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.

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.

If you do not enter an Administrator e-mail address, e-mails generated by the appliance will have the following “sender” information:

From: Network Discovery at Unknown
[mailto:email.address.not.configured@Network.Discovery]

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 6-8: Enter e-mail address



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

(Optional) Enter the SMTP server

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.

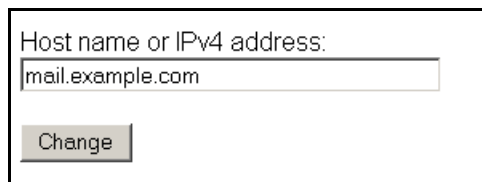
Note: You may wish to use the IPv4 address rather than the domain name of the SMTP server so that Network Discovery can still contact you even if the domain name server is unavailable.

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

To enter the SMTP server

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

Figure 6-9: Change SMTP server



The screenshot shows a web form for configuring the SMTP server. It features a text input field with the label "Host name or IPv4 address:" and the value "mail.example.com". Below the input field is a "Change" button.

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* section
- *Synchronize the time* on page 84 (or *Enter an NTP server to synchronize the time (continually)* on page 85)

Important: Make sure you set the time and date correctly. If you change the time and date later, you may lose significant amounts of data, and you may in fact have to delete all of your collected data and reconfigure your appliance.

Set the date and time

Important: If you accidentally type the year as “2004” when you meant “2003” and later have to set the year, correctly, to 2003, then Network Discovery will take one year to start updating the map again. This problem can only be rectified with the help of Peregrine customer support.

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.

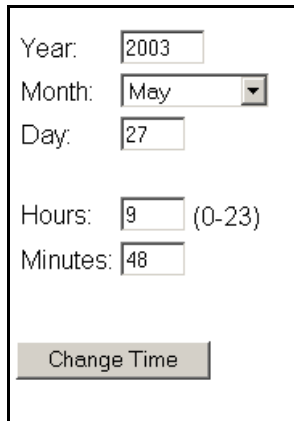
Note: Seconds are not set explicitly. When you click the Set Time button, seconds are set to 0.

To set the time and date

- 1 Make sure the time zone is set (see *Setting the time and date* on page 84).
- 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 6-10: Setting the time and date



Year:

Month:

Day:

Hours: (0-23)

Minutes:

Synchronize the time

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

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

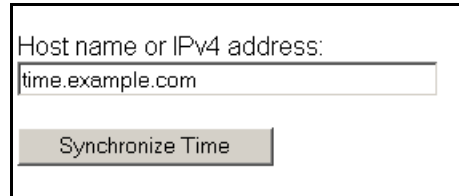
Note: The Synchronize Time option only synchronizes the time once. It does not repeatedly re-synchronize.

To synchronize the time

- 1 Make sure the time zone is set (see *Setting the time and date* on page 84).
- 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 6-11: 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.

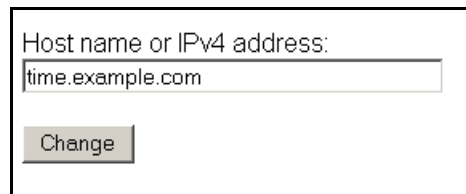
An NTP (Network Time Protocol) server is a server that keeps track of and reports the exact time. Network Discovery can synchronize its system time with the time reported by the NTP server.

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 6-12: 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

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 151.

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.)

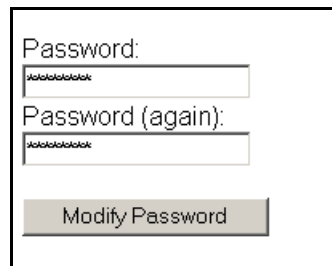
Passwords can be 4–20 characters long by default. The minimum password length can be specified in **Administration > Account administration > Appliance passwords**.

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 6-13: Changing the admin password



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

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 6-14: Enable or disable warnings

Click **No** to disable a warning that you do not have recommended equipment

<u>UPS warnings enabled:</u>	<input type="radio"/> Default: Yes
	<input checked="" type="radio"/> Custom: <input type="radio"/> Yes <input checked="" type="radio"/> No
<u>Modem warnings enabled:</u>	<input type="radio"/> Default: Yes
	<input checked="" type="radio"/> Custom: <input type="radio"/> Yes <input checked="" type="radio"/> No
<u>Backup warnings enabled:</u>	<input type="radio"/> Default: Yes
	<input checked="" type="radio"/> Custom: <input type="radio"/> Yes <input checked="" type="radio"/> No

Click **Change**

Change

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** > **System preferences** > **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** > **System preferences** > **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* (visible at the bottom of the Health Panel).

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 > System preferences > Display warnings**
- 2 For Backup warnings enabled, click **Yes** or click **No**.
- 3 Click **Change**.

7 Licenses

CHAPTER

Peregrine Systems makes increased functionality available through license files you can install once you receive them from Peregrine Customer Support.

[Request a new License](#)

[Install the new license](#)

How it works

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

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, including up to five PDI scanned devices
- 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.

Evaluation License

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

Disaster Recovery License

If your appliance breaks, you can get a disaster recovery license (at no cost). This license will allow you to backup your data to a new appliance. Then, you will be able to use the new appliance for up to 30 days, while your old appliance is being fixed. You can restore your data a total of 3 times while using this license.

Basic Discovery License

Basic Discovery means that Network Discovery will only discover devices on your network. Network Discovery will not monitor those devices.

Once you have installed your Basic Discovery license, you should change the “Basic Discovery” setting at **Administration > System preferences > Appliance services > Force Basic Discovery mode**.

This option will turn off the following user interface elements:

- Network Map
- Service Analyzer
- MIB Browser

It will also disable the following internal processes:

- Device poller
- Resource poller
- Environment poller
- Mapping engine (connectivity)

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.

You can send a request for a new license in two ways:

- The Peregrine appliance can send an e-mail message directly to Peregrine Systems Customer Support.
- You can copy the information into an e-mail and send the e-mail manually.

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

- 1 Administration > Appliance management > Generate licensing request.**
- 2 Complete the form. Be sure to select one of the three license types:**
 - a Basic Discovery**
 - b Network Monitoring**
 - c Aggregation**
- 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.

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.**

To install the new license

- 1 Click **Administration > Appliance management > Install license.**
- 2 Click the **Browse...** button to locate the license file sent to you by Peregrine Systems.
- 3 A **Choose File** window appears.
- 4 Find and select the license file.
- 5 Click **Open.**
- 6 Click **Submit.**

8 Set up Network Discovery

CHAPTER

The following flowchart shows all the important tasks that must be completed to set up Network Discovery. There are other optional tasks described throughout the chapter.



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.

Important: If you are using Network Discovery with Desktop Inventory, you must follow the steps outlined in *Using Network Discovery with Desktop Inventory and Desktop Administration*.

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 107.

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

Run router discovery

Router Discovery is a tool you can use to automatically locate the SNMP-managed routers and subnets in your network. Network Discovery will give you a list of routers, and you can use that list to populate your IPv4 ranges while setting up Network Discovery.

Router Discovery only runs when you initiate it. This is not a continuous process.

If you would rather enter your IPv4 ranges manually, go to *Set up the IPv4 range(s) to discover* on page 98.

Set up Router Discovery

- 1 Click **Administration** > **Router discovery** > **Router discovery settings**.
- 2 Set the community strings, maximum hops, minimum and maximum line speeds.

Note: The list of community strings must be separated by commas (for example, “public,private,string1,string2”).

- 3 Click **Change**.

Note: Hop 0 (zero) is always the Peregrine appliance itself, and hop 1 is always the default gateway.

Run Router Discovery

- 1 Click **Administration** > **Router discovery** > **Run router discovery**.
- 2 Click **Confirm**.

You will receive an e-mail confirmation when Network Discovery has completed the router discovery process. At that point, you can apply the results to your IPv4 range.

Apply the Router Discovery results to your IPv4 Range

- 1 Click **Administration** > **Router discovery** > **Router discovery results**.
- 2 Choose a property set for each discovered router (typically, you should choose the “Active Discovery” option).
- 3 Click **Add to IPv4 Ranges**.

Set up the IPv4 range(s) to discover

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

Import your IPv4 ranges from a CSV file

Instead of entering all your IP ranges manually, you can import them from a CSV file. The file must be set up properly, as in the example below.

State whether this is a range or a subnet Starting IP address Ending IP address or netmask Define whether this is a Property Group or Property Set (Set, Network, Community, Scanner, Listener) The name of the Property Group or Property Set you've specified in the previous column. The name must be exactly as it appears in the Network Configuration page.

	A	B	C	D	E	F
1	range	172.22.2.5	172.22.2.56	Network	global	
2	subnet	172.22.9.5	255.255.255.0	Set	global	
3						
4						
5						
6						
7						
8						

testimport

To import IPv4 ranges from a CSV file

- 1 Click **Administration > Network configuration > Import IPv4 Range Definitions**.
- 2 Click the **Browse** button to select your CSV file.
- 3 If you wish to delete your existing IPv4 ranges before you import the CSV file, click **Yes**.
- 4 Select a default Property Group/Set.

Note: If you have not specified Property Groups/Sets in your CSV file, you can choose one to apply to all of your IPv4 ranges. If you have specified Property Groups/Sets for some of the IP ranges in the CSV files, the ones in the CSV file will take precedence. If you do not specify Property Groups/Sets in the CSV file, and you do not select a default, the IP range will not be imported.

5 Click **Import**.

Once you import the CSV file, you will see a report explaining whether or not the import was successful. Read the report carefully to ensure that all your IPv4 ranges have been imported properly.

Note: By default, Network Discovery will insert the “global” IPv4 range of 0.0.0.0 - 255.255.255.255, even if you have not listed it in your CSV file.

View an IPv4 range

Note: If you have run Router Discovery, the IPv4 ranges you added in the previous procedure should also appear in this list.

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 your *Pre-setup Questionnaire*.

Export your IPv4 ranges to a CSV file

You can export a CSV file as a way of keeping an external record of your IPv4 ranges. Also, you can modify the configuration in the CSV file and then “import” them.

To export the IPv4 ranges

- 1 Click **Administration > Network configuration**.
- 2 On the **List IPv4 Ranges** line, click **CSV Export**.
- 3 Save the file.

Delete an IPv4 range

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

To delete an IPv4 range

- 1 From **Administration > Network configuration > List IPv4 ranges**.
- 2 Select the IPv4 range.
If the range has subranges, Network Discovery gives you a choice of deleting only the range or of deleting the range plus all of its subranges.
- 3 Click **Delete this IPv4 range**.
- 4 Click **Delete**.

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

Add an IPv4 range

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

Note: If you add an IPv4 range that is 65536 or more devices, you will see a warning message. The warning is only there to guard against possible errors when you are configuring your IPv4 ranges. Network Discovery will still operate normally if you choose to use IPv4 ranges of that size.

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.
Note: If you prefer, you can also enter a single octet netmask (for example, enter an IPv4 address of 172.22.1.1, and a Netmask of 24). To enter a range for one address, you can enter the IPv4 address, and a netmask of 32.
- 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 step 1 to step 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 addresses 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. (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 107.

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. If you are unsure of why some devices are appearing, and other devices are not appearing, here are some suggestions to help you investigate.

Peregrine Systems recommends waiting at least 48 hours while Network Discovery is first discovering your network. If you have concerns after that, call customer support.

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 Click **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 list for any problems. The Exceptions list 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 network changes.

To see a list of the Exceptions

- ▶ On the Health Panel, double-click the **Exceptions** alarm category. The Alarms Viewer will open, listing all the devices that have exceptions. You can open a Device Manager for any of the devices to see if there are any other problems.

Check the Device Filters report

There may be devices on your network that do not appear on the Network Map because the devices are being filtered. To check if any devices are being filtered out, check the Device Filters report.

To check the Device Filters Report

- ▶ Click **Status > Filtered devices**

To see a full list of possible filters, click **Help > Classifications > Device Filters**.

Check the Device Modeling Queue

During the initial discovery of your network, the modeling queue may show devices, depending on the size of your network and how quickly Network Discovery is discovering and modelling devices. At most other times, the queue will be empty.

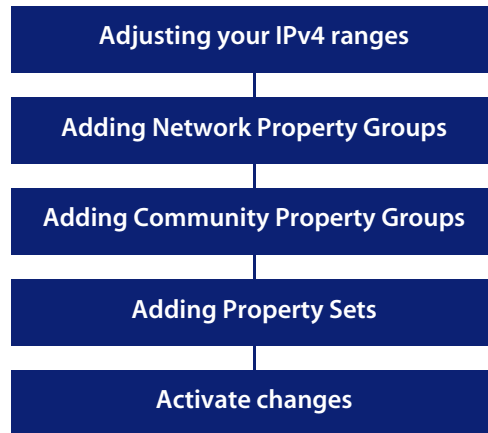
To check the Device Model Status Report

- 1 Click **Status > Network model queue** to view the devices that are waiting to be network modeled.
- 2 Click **Status > Network model processing** to view the devices that are in the process of being network modeled.

9 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.



A precise matrix of network discovery

In chapter 8, *Set up Network Discovery* on page 95, 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, pages printed information from printers, or battery levels from UPSs.

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 9-1: 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
--[172.22.1.1 to 172.22.1.3]	Network: Active discovery
--[172.23.0.0 to 172.23.15.255]	Network: Active discovery
--[172.23.0.3 to 172.23.0.3]	Network: Unmanaged router
--[172.23.0.4 to 172.23.0.9]	Network: Do not allow discovery
--[172.23.0.4 to 172.23.0.5]	Network: Resource/Environment manage

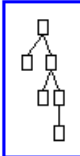
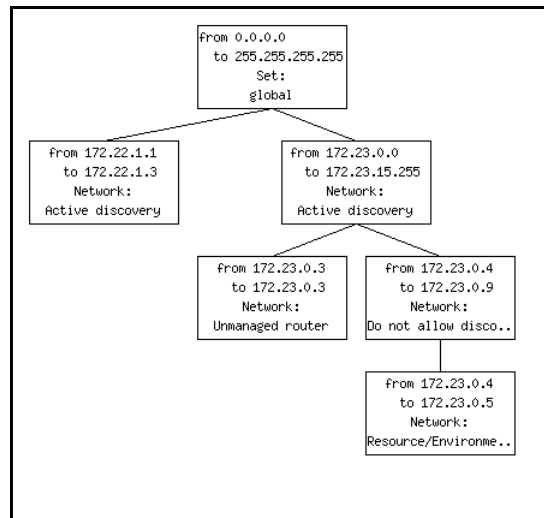


Figure 9-2: Example of a developed network tree as shown in “Review changes”



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.

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
- Scanner—for Scanner deployment
- Listener—for Listener deployment

Note: To set up Scanner and Listener Property Groups, see *Using Network Discovery with Desktop Inventory and Desktop Administration*.

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.

Here is a list of default Network Property Groups:

- global
- Active discovery
- Do not allow discovery
- Resource/Environment manage
- Do not resource manage
- Unmanaged router
- DHCP server
- Restrict to scanned-only
- All off
- Passive discovery
- Remove address

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.

You can change any of the Network Property Groups, or add your own as you become better acquainted with Network Discovery. It is important to understand that Network Discovery has a series of hardcoded default settings for these properties, and the user cannot change them. This means that even the “global” property group can “inherit” settings from this hardcoded list.

The following properties are in every Network Property Group:

Table 9-1: Default Network Properties

Property	Purpose	Hardcoded Default Setting
Allow devices	Allow devices to be added	Off
Actively ping	Actively ping devices for discovery	Off
NetBIOS query	Query devices for their NetBIOS names (the computer user names)	Off
Resource/Environment manage	Query devices for resource management	Off
Force ARP table read	Force ARP table to be read	Off
Accumulate IP Addresses	Accumulate IP addresses instead of replacing them	Off
Allow IP addresses	Set to Off 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 On when you want to allow the repeated IPv4 addresses to be included.	On

Table 9-1: Default Network Properties

Property	Purpose	Hardcoded Default Setting
Allow ICMP and SNMP	<p>Pinging and polling is turned off, so devices will not be modelled. If the device is already in the database, Network Discovery will still poll and ping the device for other reasons (for example, to monitor device attributes).</p> <p>Although pinging and polling is turned off, devices can still be discovered by PDI and included in the database.</p>	Off
Device modeler interval	<p>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.</p>	172800 seconds (48 hours)

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 and cause more load on the device being monitored. 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 9-2: 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. Provides disk, CPU, and memory information from servers, printers or UPSs.
Unmanaged router	In this Property Group, Accumulate IP addresses is set to “on”. For routers that do not have SNMP management enabled.
DHCP Server	This Property Group has Force ARP table read set to “on”. For servers providing Dynamic Host Configuration Protocol (DHCP) services, or for any other device (except routers) with a large ARP cache.

Table 9-3: 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	Use it as a “child” range of a Resource Manage range.

Table 9-3: Default Network Property Groups that decrease functionality (and traffic)

Property Group	Purpose
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 Peregrine Desktop Discovery (PDI).
Remove Address	Used for removing IP addresses from the device model.
All off	The least active of the default Property Groups. 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 Click **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**.

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**.

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.

Note: Community strings are the only property associated with an IP range that does not allow inheritance.

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).
- 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.

When you add community strings, the order is important, make sure the most frequently used strings are at the top of the list.

- 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.”

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 to the system 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 SNMP QUERY 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 IPv4 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.

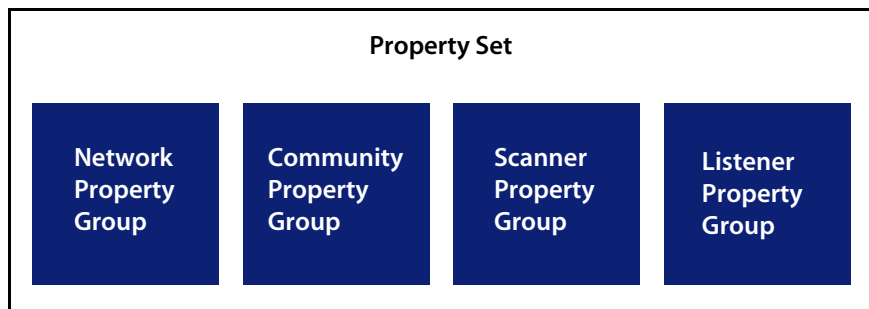
To delete a Community Property Group

- 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” can contain 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 should always give your Property Sets meaningful names, for example “servers” or “routers” so you can apply it to specific portions of your network.

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

Figure 9-3: Default Property Sets

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

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 8. 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 to ping each address scheduled for active discovery (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. Removed ranges are in grey.

- 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**.

10 Setting up 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.

There are four pre-installed accounts

Network Discovery comes with four accounts pre-installed, one each of the following types:

- Demo
- IT Employee
- IT Manager
- Administrator

The Network Discovery Administrator must create all other accounts.

Figure 10-1: List of pre-installed accounts

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

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
- Scanner—exclusively used to upload scan files from Desktop Inventory.

For a full list of account properties and capabilities, see the *Network Discovery User Guide*.

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.

Creating accounts

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

You should also modify the capabilities of the account and the contact data for the person who owns the account.

You can also modify the properties of the account, but 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 3-16 characters long. Acceptable characters are:

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

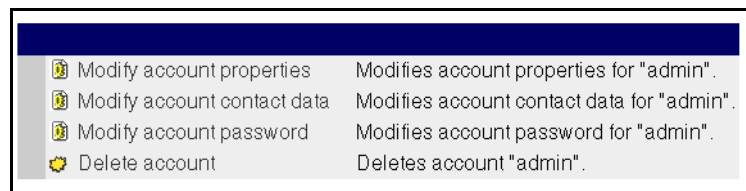
- 3 Click **Add Account**.

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 10-2: Brief menu for adding an account



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

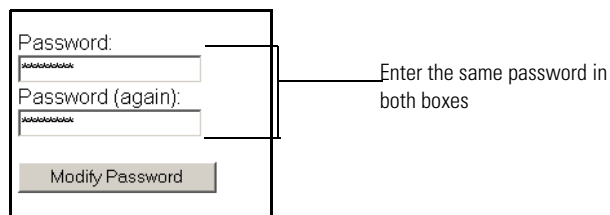
To create a password for an account

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 10-3: Entering an account password



The image shows a user interface for changing a password. It features two text input fields. The first field is labeled "Password:" and the second is labeled "Password (again):". Both fields contain masked characters (asterisks). Below the fields is a button labeled "Modify Password". A line points from the text "Enter the same password in both boxes" to the right side of the two input fields, indicating that the passwords must match.

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

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

To change an account type

- 1 Click **Administration > Account administration > Account capabilities**.
- 2 Select the account from the list box.
- 3 Click **Modify Capabilities**.
- 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 capabilities, as appropriate.
- 6 Click **Modify Capabilities**.

(Optional) More Account Administration

There are other account settings you may want to set. For more information on these topics, see the User Guide, or read the help information associated with each feature in **Administration > Account administration**.

Feature	Description
Appliance passwords	These are global settings for all account passwords. Change the length of passwords, password history, and the number of allowed login attempts.
Account capabilities	These settings control the account type, the access to Network Discovery components, and password expiry. Only Administrator users can access this menu.
Account properties	These settings control how the user will view data in Network Discovery.

Note: You can make changes to your own account at **Administration > My account administration**.

11

CHAPTER

Backup and Restore

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 132
- *Choosing tape or an FTP site for your external backup* on page 133
- *Configuring an external backup* on page 134
- *Testing your external backup and restore* on page 136
- *To run an internal or external backup immediately* on page 138
- *Restoring your data* on page 139

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 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.

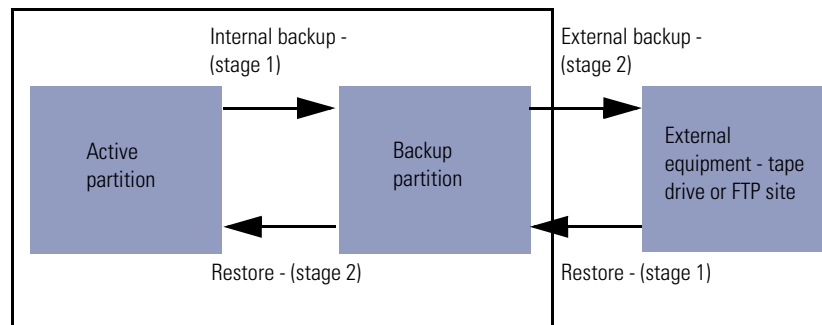
If you decide to store external backups, Network Discovery performs two separate functions. Every day, after midnight, Network Discovery creates an internal backup. Once the internal backup is complete, Network Discovery sends that internal backup to the FTP site and/or to the USB tape drive.

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

Important: After a restore, there may be phantom alarms on the Health Panel and in the Alarms Viewer for the first sampling period, because the events log has been affected by restoring from an old backup.

Note: Both the backup and restore functions must go through the intermediate backup partition. You cannot backup directly from the active partition to an external site, and you cannot restore from the external site to the active partition.

Figure 11-1: 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 and Windows 98 running IIS
- Windows NT Server (IIS)
- Windows 2000 Professional (IIS 4)
- Red Hat Linux: Kernel 2.2.12, ProFTPD version 1.2.6

For a recommended USB tape drive, see [Appendix C, Extra Hardware](#) on page 155.

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

External backups are made approximately every 24 hours, some time after midnight, and after the internal backup. If the internal backup fails, the external backup will not proceed.

Note: External backups are not scheduled until the Peregrine appliance has been in use for at least 2 hours. For example, if you attach your Peregrine appliance to your network at an hour before midnight, or 2300 (11 PM), and request an external backup, the backup cannot begin until 0100 (1 AM).

Note: If a backup fails, Network Discovery generates an e-mail (assuming Network Discovery is configured to allow this). Network Discovery waits approximately 30 minutes, then tries again to create a backup. Each failure generates a new e-mail.

Procedural alerts

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.

- For FTP, it is your responsibility to ensure that the username, password, host name or IP address, directory, filename and port are all valid. You should test your backup (*Testing your external backup and restore* on page 136), every time you make a change.
- The e-mail option will work if:
 - a DNS server has been configured (see *Enter the domain name server* on page 77)
 - the Peregrine appliance is connected to the internet
 - the e-mail address is provided

- the account contact data includes an e-mail address

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**.

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.

Note: If you create a filename containing illegal characters, the backup will fail.

- *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. (Scan files will take up a lot of space.)
- 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).

For tape backup/restore, Network Discovery checks:

- whether a tape drive can be found
- whether a tape is in the drive

For FTP backup/restore, Network Discovery checks:

- the existence of the device specified
- whether the username and password work for the device
- the port specified for the device
- read/write ability for the device

For appliance restore, Network Discovery checks:

- the connection to the second Peregrine appliance

- that the second Peregrine appliance can provide data
- that the data on the second Peregrine appliance is compatible with the active appliance

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 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 check the Test Backup Log

- 1 Click **Administration > Backup and restore > View test log**.
- 2 Select a test log from the Test Results list.
- 3 Click **Display**.

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.

Warning: If tape backup is selected, the tape in the drive will be erased.

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

Important: Restoring overwrites the active data. This action cannot be undone.

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.

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**.
Network Discovery will not respond for a short period. This is normal.
- 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.

Important: It is your responsibility to ensure that the username has read/write permission for the FTP directory.

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

This procedure is useful for migrating data from one Peregrine appliance to another. If one appliance has been damaged, you should use this procedure to move your data to a new appliance.

The following list offers a summary of the tasks you need to perform.

- *Step 1: Setup your new Peregrine appliance*, but do not connect it to the network.
- *Step 2: On your old appliance, do an internal backup*
- *Step 3: Connect the crossover cable between the two appliances*
- *Step 4: Check the connection between the two appliances*
- *Step 5: Remove the old appliance from the network*
- *Step 6: Connect the new appliance to the network*
- *Step 7: Log in to the new appliance*
- *Step 8: Restore on new appliance*

Step 1: Setup your new Peregrine appliance

Perform the procedures as detailed in this *Setup Guide*, [Chapter 5, Install and Start Network Discovery](#). If your new appliance will have the same IP address as the old appliance, do not connect the new appliance to the network yet. You will do that later in this process.

Step 2: On your old appliance, do an internal backup

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

If you cannot perform this step, you will restore data from the last time the old appliance did an automatic internal backup (which occurs daily after midnight).

Note: This action will also initiate an external backup if one has been configured.

Step 3: Connect the crossover cable between the two appliances

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

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

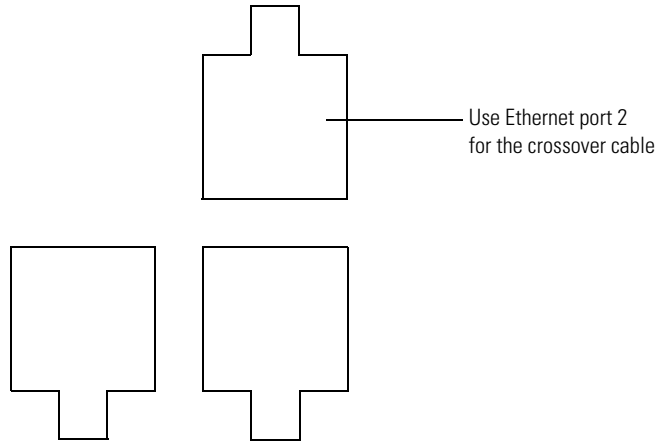


Figure 11-3: Ethernet port 2 on the IBM xSeries 330

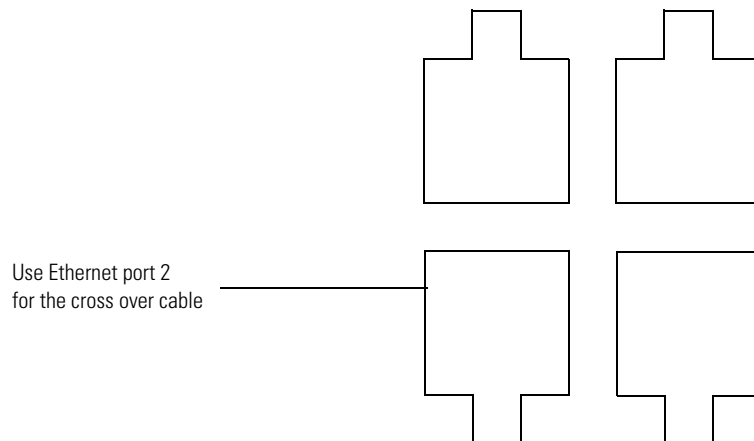
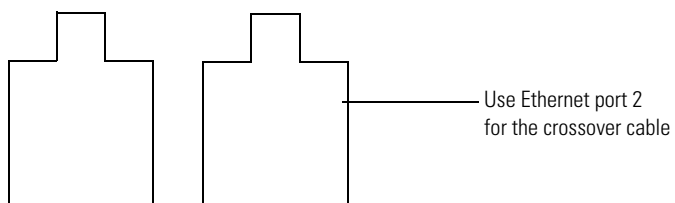
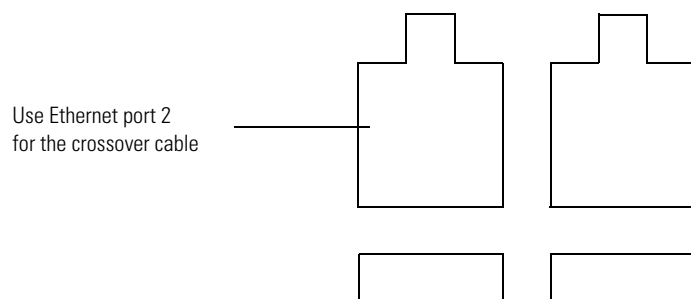
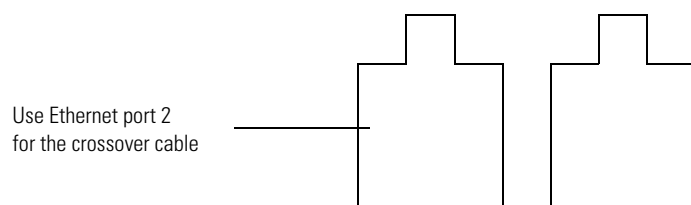


Figure 11-4: Ethernet port 2 on the Dell 1750**Figure 11-5: Ethernet port 2 on the Dell 1650/2650****Figure 11-6: Ethernet port 2 on the HP DL360/DL380**

Step 4: Check the connection between the two appliances

To check the connection between the two appliances

- 1 On the new appliance, click **Administration > Backup and restore > Test external backup and restore**.
- 2 Select “appliance.”
- 3 Click **Test**.

Step 5: Remove the old appliance from the network

- ▶ Disconnect the network cable from the old appliance.

Step 6: Connect the new appliance to the network

- ▶ Follow the procedure *Connect the appliance to the network* on page 59 in *Chapter 5, Install and Start Network Discovery*.

Step 7: Log in to the new appliance

- ▶ Enter the URL for your appliance and log in with the following info:
User Name: admin
Password: password

Step 8: Restore on new appliance

To restore your data from another appliance

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

When you click **Restore**, the copy is scheduled for one minute later. The data will be copied to this Peregrine appliance as a backup, then the backup replaces the active data for this appliance.

Note: Your accounts will be restored from the backup, so you will be prompted to login again.

12 Shutting down the Peregrine Appliance

CHAPTER

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.

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 57.

To shut down the Peregrine appliance—through the browser interface

- 1 Administration > Appliance Management > Appliance Shutdown.
- 2 Click **Shut down appliance**.
- 3 When the text “The system is halted” appears on the screen, power off the Peregrine appliance.

The Peregrine appliance shuts down safely.

A Before you call...

APPENDIX

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 148
- *Check that your maintenance license is current* on page 148
- *Check that you have the latest software components* on page 148
- *Download the new component(s)* on page 149
- *Install the new component(s)* on page 149
- *After you install new components* on page 150

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 (support.peregrine.com) to 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.

- 4 From the pull-down list, select **Query Network**.

- 5 Click **Update**.

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.

B 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 26 and *Enable firewall ports* on page 28.

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

This is a documented community string, known to:

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

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

There is more information in *Change the Peregrine appliance community strings* on page 75.

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

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

These are documented account names, known to:

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

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

There is information about accounts in Chapter 10, *Setting up Accounts* on page 125.

- 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 10, *Setting up Accounts* on page 125 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:

- Admin 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 54.

C 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 or Dell 1650 version of the Peregrine appliance to increase its capacity from a maximum of 4,000 to a maximum of 8,000 devices.

You can add a second CPU to an IBM xSeries 335 or Dell 1750 version of the Peregrine appliance to improve its performance.

Any new processor must match the existing processor in your Peregrine appliance.

You can add an internal modem to the IBM xSeries 335 or the IBM xSeries 330, Dell 1750, Dell 1650, or HP360. 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 and initialize the new hardware configuration.

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 *Compatibility Matrix* on page 33. 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 (**Administration > Appliance Management > Appliance Restart**).

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 45
- account
 - change type 129
 - create a password 128
 - creating 127
 - how many can access Network Discovery 126
 - pre-installed 126
 - setup 125
 - types
 - Administrator 127
 - Demo 127
 - IT Employee 127
 - IT Manager 127
- activate changes 104
- Administrator account 127
 - password, changing 86
- alarms
 - turn off *see* disabling warnings
- appliance system variables 74

B

- backup
 - FTP 133
 - immediate 138
 - external 138
 - internal 138
 - tape 133, 157
 - test 136
- backup warnings

- enable/disable 89
- Basic Discovery license 92
- BIOS boot sequence 46
- bridge aging 24

C

- CD
 - software installation 53
- Central Processing Unit *see* CPU
- changes, activating configuration changes 123
- CIR values 32
- Cisco devices 31
- collecting information 13
 - questionnaire 11
- color settings 40
- Committed Information Rate values 32
- Community Property Groups 117
- community strings
 - about 23, 119
 - changing Peregrine appliance 75
 - deleting 121
 - directed 23, 120
 - Global Community Property Group 103
 - multiple strings 119
 - SNMP traps 120
- components
 - see* software components
- configuration interface 44
- connecting power 45
- CPU
 - adding later 158

customer support access 15

D

data backup 157
 connect hardware 64
 date and time
 setting 83
 synchronizing
 continually 85
 once 84
 Dell 1650 61
 Dell 1750 60
 Dell 2650 61
 Demo account 126
 device filters report 106
 device model status report 106
 DHCP 17, 23
 servers 102
 static address for Peregrine appliance 14
 directed community strings 23, 120
 disabling warnings 87–89
 about 87
 Disaster Recovery license 92
 disaster recovery license 92
 Domain Name Server, entering 77
 domain search order, entering 77
 Dynamic Host Configuration Protocol *see* DHCP

E

e-mail
 Peregrine appliance administrator, changing
 81
 e-mail address
 blank, consequences of 135
 Evaluation license 92
 Exceptions reports 105
 external modem 157

F

firewall ports 28–30
 customer service access 26
 Frame Relay, set up 32

G

gateway 54

H

hardware
 connect keyboard and monitor 44
 extra 155
 CPU 158
 external modem 157
 internal modem 158
 tape drive 157
 UPS 155
 Home page 72
 Host name, entering 79
 Hot Standby Routing Protocol *see* HSRP
 HP DL360/DL380 51, 61
 HSRP 22

I

IBM xSeries 330 60
 IBM xSeries 335 59
 installation
 before you install the Peregrine appliance 9
 BIOS boot sequence 46
 checking the management workstation
 connect appliance to the network 59
 Dell 1650 61
 Dell 1750 60
 Dell 2650 61
 hardware
 CPU 158
 external modem 157
 extra 155
 tape drive 157
 UPS 155
 HP DL360/DL380 61
 IBM xSeries 330 60
 IBM xSeries 335 59
 preparing the network 21
 software 53
 software setup 67
 Internet Explorer
 minimum version 40
 IPv4 address 14
 of the appliance 54
 IT Employee account 126
 IT Manager account 126

J

- Java
 - enable 40
- JavaScript
 - enable 40

L

- license 91–94
 - basic discovery 92
 - default 92
 - disaster recovery 92
 - Evaluation 92
 - install 94
 - maintenance 92
 - check if current 148
 - request 93
- listener configuration 31
- log on, initial 68

M

- managed device
 - definition 14
- management console *see* management workstation
- management workstation 40
 - connect 62
 - requirements
 - browser 40
 - CPU 40
 - memory 40
 - video 40
- merge IPv4 addresses 110
- modem
 - external 157
 - internal
 - adding later 158
- modem warnings
 - enable/disable 88
- multiple community strings 119

N

- netmask 54
- Netscape, minimum version 40
- network cable 59
- network configuration 95–123
 - add DHCP servers 102

- add IPv4 range 98, 100
- add unmanaged routers 102
- apply changes 123
- community strings 103
- delete IPv4 ranges 100
- Property Groups 110
 - review and activate changes 104
- reviewing and activating changes 123
- router discovery 97
 - set up IPv4 ranges to avoid 101
- troubleshooting 105
- network discovery 95–123
- network preparation 13
- Network Property Group
 - apply to a range 117
 - create 115, 116
 - delete 116
 - modify 115
- Network Property Groups 111–117
- node and subnode setup 14
- NTP server 85

P

- paging
 - connect hardware 64
 - external modem 157
- password
 - change Peregrine appliance default 55
 - changing for Administrator 86
 - create 128
- Peregrine appliance
 - administrator e-mail address, changing 81
 - community strings, changing 75
 - no response after changing domain name server 78
 - shutdown 145
- Peregrine Systems Customer Support
 - access 15
 - access options 26–30
 - Internet 26
 - Remote Access Server 27
 - telephone line 27
 - Virtual Private Network 27
- power
 - connecting 45

- pre-installation 9
 - checking the management workstation 40
 - preparing the network 21
 - questionnaire 13
- pre-installed accounts 126
- preliminary work 10
- preparation 10
- preparing the network 21
- Pre-setup Questionnaire 13
- Property Groups 110
- Property sets 122
- proxy server 26

Q

- questionnaire 13

R

- RAS 27
- Remote Access Server 27
- requirements
 - management workstation
- resolution 40
- restore 139
 - another appliance 141
 - FTP backup 140
 - internal backup 139
 - tape backup 140
- review and change configuration 123
- router discovery 97
- routers
 - listener configuration 31

S

- screen resolution 40
- security checklist 151
- setting the date and time 83
- setting the time zone 76
- setup 10
 - give appliance its network information 54
- setup questionnaire 11
- setup, software 67
- shut down Peregrine appliance
 - browser interface 145
 - configuration interface 57
- SMTP Server, entering 82

SNMP

- traps 120
- turn on
 - in network devices 22
 - in routers and switches 22
- SNMP management
 - definition 14
- software
 - installing 53
- software components 147–150
 - check if latest 148
- software setup 67
- software upgrades 147–150
- specifications
 - management workstation
- synchronizing the date and time 84, 85
- system contact, assign 74
- system location, assign 74
- system name, assign 74

T

- tape drive 157
- telephone line 27
 - connecting appliance 65
- terminal emulation software 66
- time and date
 - setting 83
 - synchronizing
 - continually 85
 - once 84
- time zone, setting 76
- Toolbar, main 73
 - banner 73
 - status window 73
- top-of-the-network device 59
- traps, SNMP 120
- troubleshooting
 - at startup 105
 - Exceptions reports 105
 - when logging in 69

U

- unmanaged routers 102
- upgrading software 147–150
- UPS 155

acceptable units 156
connecting 63
warning, enable/disable 88, 89

V

Virtual Private Network 27

W

workgroup name, entering 80

