Peregrine

Network Discovery

Preparing for Installation

PART NO: PND-5.0.1-ENG-01011-00284

Peregrine SYSTEMS®

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

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

This edition applies to version 5.0.1 of the program, Peregrine's Network Discovery.

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

Peregrine SYSTEMS®

Network
Discovery
Preparing for
Installation

Table of Contents

1 CHAPTER Welcome to Network Discovery

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

This information in *Preparing for Installation* is critical to your success with Peregrine's Network Discovery. Your sales representative may have given it to you as a separate pre-purchase handout; or you may be seeing it for the first time as the first three chapters of the *Network Discovery Setup Guide*. The information is exactly the same. If you have seen the information before and have already done the preparation, you can go to Chapter 5, *Install and Start Network Discovery* of the *Network Discovery Setup Guide*. If you are seeing this information for the first time, let's get started.

Important: If you are upgrading from InfraTools Network Discovery (IND) 4.2 or 4.3, see chapter *12 To Upgrade from InfraTools Network Discovery or from Xanadu 1.0.4* on page 117 of the *Network Discovery Setup Guide*. Instructions for upgrading from Network Discovery 5.0 are in the 5.0.1 *Release Notes*.

About Network Discovery

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

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

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

Why it’s important to prepare

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

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

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

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

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

Start by collecting information about your network

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

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

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

To find Peregrine worldwide contact information:

1 Log on with your login user name and password.

2 Click **Go for CenterPoint**.

3 Select **Whom Do I Call?** in the navigation bar on the left side of the page.

Peregrine worldwide information is displayed for all products.

You can obtain a copy of the questionnaire:

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

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

CHAPTER 2

Pre-setup Questionnaire

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 18.

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

Telephone number for access by Peregrine Systems Customer Support ______________________________

List IPv4 ranges for Network Discovery to discover

Network Discovery uses IPv4 ranges to discover the devices in your network. It works best when you give it a broad idea of where the devices in your network are—but exclude ranges where you know there are no devices.

Note: While you are making a list of devices in your networks, indicate bridges, routers, switches, and concentrators, so that you can identify them easily.

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

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

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

List IPv4 ranges for Network Discovery to avoid

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

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

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

List the community strings of your network’s devices

For an explanation of community strings, see *About community strings* on page 17.

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

Does Network Discovery need to know the write string?

- No. Network Discovery will operate without write strings. However, if you do give Network Discovery the write strings, the owner of an Administrator account will be able to manage the device from the Network Discovery interface.

		Rights granted	
Community string	Associated device /IPv4 range	Read	Write

Enter TCP/IP configuration

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

Are TCP/IP addresses static or dynamic? **Static__________ Dynamic__________**

If dynamic, enter the following:

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

____

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

Is SNMP management enabled on the DHCP server? **Yes _________ No_________**

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

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

Unmanaged router number 1 ________________________________

Unmanaged router number 2 ________________________________

Unmanaged router number 3 ________________________________

What server will you use for the Peregrine appliance?

Please check one (for more information, see *Check the server that will be the Peregrine appliance* on page 22):

Large IBM xSeries 335 ________

Small IBM xSeries 335 ________

Large IBM xSeries 330 ________

Small IBM xSeries 330 ________

Send the questionnaire

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

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

To find Peregrine worldwide contact information:

1 Log on with your login user name and password.

2 Click **Go for CenterPoint**.

3 Select **Whom Do I Call?** in the navigation bar on the left side of the page.

Peregrine worldwide information is displayed for all products.

3 CHAPTER

Prepare the network

Topics in this chapter include:

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 17.

Set DHCP lease time

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

(Optional) Turn on SNMP management in other devices

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

About community strings

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

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

Directed community strings

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

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

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

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

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

(Optional) Adjust bridge aging

To improve the reliability and speed of Network Discovery, adjust bridge aging on your bridges, routers, switches, and concentrators. Turn bridge aging on, and set the bridge aging interval to 2-6 hours. Smaller networks can use shorter intervals; larger networks will need longer intervals. Network Discovery's Exceptions reports can tell you which devices should have their bridge aging adjusted.

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

Plan to attach the Peregrine appliance:

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

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

Choose how to receive Peregrine Systems Customer Support

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

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

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

Through Internet access

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

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

Used for	Port	Note
Secure Shell (SSH)	22/tcp	
HTTP	80/tcp	
MIB browser	8100/tcp	
Network Map	8101/tcp	
Network Map proxy	8102/tcp	1,2
MIB browser proxy	8103/tcp	1
Telnet proxy	8104/tcp	1
HTTP proxy	8105/tcp	1
MySQL ODBC	8108/tcp	

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 35.

Through a Remote Access Server (RAS)

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

Enable firewall ports

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

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

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

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

Telnet proxy	8104/tcp	1	management workstation	Peregrine appliance
		1,2	Peregrine appliance	aggregated Peregrine appliance
HTTP proxy	8105/tcp	1	management workstation	Peregrine appliance
		1,2	Peregrine appliance	aggregated Peregrine appliance
MYSQL ODBC	8108/tcp	1	management workstation	Peregrine appliance
Traceroute	33263/udp		Peregrine appliance	device

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

Check Cisco devices

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

Check Committed Information Rate (CIR) values

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

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

Check the server that will be the Peregrine appliance

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

For a new installation, use an IBM xSeries 335.

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

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

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

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

Table 3-4: Specific IBM xSeries 335 hardware requirements

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

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

Table 3-5: Specific IBM xSeries 330 hardware requirements

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

Check the management workstation

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

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

Item	Required	Recommended
Web browser	Use Netscape 4.07 or later (but do not use 4.60 and do not use Netscape 6.x except 6.2.2 or later)	Netscape 4.7 or later
	Internet Explorer 5.0 or later[a]	Internet Explorer 5.0 or later
Video —colors	256[b]	65,000 or more
—resolution	800×600	1024 ×768 or more
Memory (MB RAM)	32[c]	64[d] or more
CPU	Pentium 100 equivalent	Pentium II 233 equivalent or better
Operating system		Windows 2000 or better

[a] Requires a Virtual Machine (VM) upgrade.
[b] 256 colors normally give adequate performance. However, in Netscape (with Windows 95, Windows 2000, or Windows NT), there may be unexpected colors on the Network Map.
[c] You must close all applications other than your web browser.
[d] 128 MB is recommended for large network maps.

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

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

Java Support

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

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

Peregrine SYSTEMS®

January 24, 2003