Peregrine

Network Discovery

Preparing for Installation

Version 5.2.1

PART NO: DPND-521-EN11

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 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

1 CHAPTER Welcome to Network Discovery

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 the *Setup Guide*. 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 9), 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.

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 22.

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 19.

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 29):

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

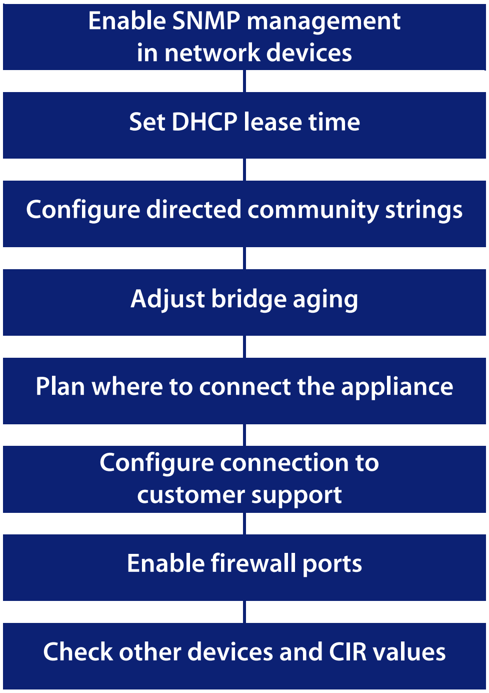
When you have completed the questionnaire, send it to Peregrine Systems Inc. by e-mail, mail or by fax. To find the mailing address or fax number of the Peregrine office in your region, contact your OEM/VAR or check http://support.peregrine.com.

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.


Enable SNMP management in network devices
Set DHCP lease time
Configure directed community strings
Adjust bridge aging
Plan where to connect the appliance
Configure connection to customer support
Enable firewall ports
Check other devices and CIR values

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 19.

(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 the *Setup Guide*.

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.

CHAPTER

4 Compatibility Matrix

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	Medium Appliance	Large Appliance
	1 CPU, 1GB RAM	2 CPUs[a], 2GB RAM	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 the *Setup Guide*.

	Small Appliance	Medium Appliance[a]	Large Appliance
	1 CPU, 1GB RAM	2 CPUs, 2GB RAM	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	■ 1650 ■ 1750 ■ 2650
IBM	IBM 335 ■ 8676-11x ■ 8676-21x ■ 8676-61x ■ 8676-81x ■ 8676-J1X IBM 330 ■ 8674-41x
HP	HP DL360 ■ 337054-001 HP DL380 ■ 293765-001

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 —colors	16,000	65,000 or more
—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.**

Index

Peregrine
SYSTEMS®