

Peregrine

Network Discovery

Release Notes

Version 5.1

Copyright © 2003 Peregrine Systems, Inc. or its subsidiaries. All rights reserved.

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

Peregrine Systems® and ServiceCenter® 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 5.1 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

Overview	8
Hardware and Browser Requirements	9
Visible improvements.	10
Three types of change alarms	10
Opening ServiceCenter tickets	10
Desktop Inventory awareness	10
Inventory Only Mode	10
IPv6 support	11
Aggregator	11
General UI improvements.	11
Toolbar	11
All Applets	12
Network Map	13
Health Panel	16
Alarms Viewer.	18
Exceptions Report	18
Service Analyzer	19
Events Browser	19
MIB Browser	20
Find	20
The Managers	20
Device Manager	21
Port Manager	23
Attribute Manager	24

Administration Menus	24
Basic Administration	24
Notification and Events Configuration	25
Advanced Administration	26
Status	27
Reports.	28
Download	29
Help	29
Device and Port properties	29
Alarm Threshold Defaults	30
Forecast	31
Deactivation	31
Hidden Devices	32
Reactivation.	32
Database Schema	32
Internal improvements	34
Appliance changes	34
Network Explorer	35
Device modelling	35
Environmental poller	36
Table reader.	37
Broadcasts	38
Virtual device handling	38
Break handling	38
Alarm Reports.	39
Ports License	39
New Line Alarm Types	39
Updated device scripts	39
Updated device rulebase	40
Miscellaneous	40
Upgrade/Migration information	41
Upgrading from Peregrine's Network Discovery 5.0, 5.0.1, or 5.0.2	42
Migrating from InfraTools Network Discovery 4.2 or 4.3.	43
Migrating from Xanadu.	43
After an upgrade.	43

Documentation	43
Dropped functionality	44
Known issues	45
Corrected issues	47
Need more help?	48
Peregrine's CenterPoint Web Site.	48

Network Discovery 5.1

Release Notes

The version 5.1 release of Peregrine's Network Discovery is a minor release of the product. This release corrects a number of issues, and adds a lot of functionality.

These *Release Notes* for version 5.1 have the following sections:





- *Overview* on page 8
- *Hardware and Browser Requirements* on page 9
- *Visible improvements* on page 10
- *Internal improvements* on page 34
- *Upgrade/Migration information* on page 41
- *Documentation* on page 43
- *Dropped functionality* on page 44
- *Known issues* on page 45
- *Need more help?* on page 48

Overview

Network Discovery 5.1 introduces many new features in relation to monitoring and event generation of device and port attributes.

In all previous versions of Network Discovery, the Health Panel, Network Map and Events Browser had a fixed set of questions that could be displayed. In ND 5.1, these components have been completely redesigned to support an expanded set of questions. These questions are now called “alarms”. The full list of what is alarmable is available in **Help > Classifications > Alarms**, but the list now includes things such as Disk, Memory and CPU Utilization, Battery Capacity and Exceptions.

In previous versions of Network Discovery, the questions on the Health Panel and Network Map had a severity of “alarm”, “warning”, or “ok”. The events browser also had “info”. In Network Discovery 5.1, these severities have been made consistent and there is now an expanded set. “Severity” has also been renamed “State”.

Previous Versions	Version 5.1	Indicator	
n/a	n/a (not an alarm state, this indicates that the attribute is not being monitored)		blank
OK	OK	—	dash
Info (was in Events Browser only)	Info		green asterisk
Warning	Minor Alarm		gold triangle
Alarm	Major Alarm		orange diamond
—	Critical Alarm (new concept in Network Discovery 5.1)		red square

In previous versions of Network Discovery, you could change the alarm colors. This is no longer possible. The colors are standard, and apply to all features of Network Discovery, including the circles on the Network Map that indicate object and line alarm status.

In addition to generating Events on an expanded list of attributes, events can now be generated on device and port property changes, as well as device and port moves (aka connection changes). Events can be natively integrated into ServiceCenter via the event filters.

Hardware and Browser Requirements

For the management console, the recommended memory has been changed to 512 MB of RAM, and the recommended CPU is a Pentium III 800 equivalent or better. The minimum required video colors is now 16,000.

The following components have been converted to Swing-based Java GUI: Health Panel, Network Map, Alarms Viewer (replaces health panel reports), Events Browser, MIB Browser and Service Analyzer. To support this Java requirement, the browser requirements have been changed.

Network Discovery 5.1 supports only the following browsers:

- Netscape 6.2.2 or later
- Internet Explorer 5.5 or later

You must install Java Runtime Engine 1.4.1_01 or later, and it must be downloaded from java.sun.com. Do not use the version that comes with your browser.

Note: You can find Java Runtime Engine 1.4.2 in the Download page of Network Discovery, the file is called “j2re-1_4_2-windows-i586.exe”.

Visible improvements

Three types of change alarms

In earlier releases, Change alarms on the Health Panel could be an “add” alarm, a “move” alarm or a “not recently seen” alarm. In Network Discovery 5.1, there are now 3 separate categories on the Health Panel and in the Alarms Viewer.

In 5.1, the term “change” refers to “property changes” such as changing a device icon, which is a new alarm on the Health Panel.

Opening ServiceCenter tickets

Network Discovery can now automatically open, update, close, and re-open tickets in Peregrine ServiceCenter.

You can set up event filters to open the tickets, and can see the ticket numbers on the Network Map, as well as in the Device Manager, Alarms Viewer, and Service Analyzer. Network Discovery will not display or modify other ServiceCenter tickets.

Network Discovery will work with ServiceCenter 5.1 or later (without requiring any ServiceCenter unloads).

Desktop Inventory awareness

Network Discovery is now aware of Desktop Inventory. Network Discovery can accept scan files from Desktop Inventory and can deploy Desktop Inventory scanners using the Desktop Administration agent.

For more information, see *Using Network Discovery with Desktop Inventory*.

Inventory Only Mode

This is a new user preference to make the product work similarly to the way IND 4.x worked in the Automated Inventory marketing bundle.

You can use Inventory Only mode to remove polling traffic from the network. When used with Desktop Inventory, this provides powerful features.

Map functions are disabled in Inventory Only mode. Unlike Automated Inventory in 4.x, the Health Panel and Alarms Viewer are enabled in this mode so that Add events, Delete events, and exceptions are visible.

IPv6 support

The Network Discovery user interface is entirely IPv6 enabled, except for telnet and HTTP proxies and the Asset Viewer.

Aggregator

You can now aggregate up to 10 Peregrine appliances, up to a total of 50,000 devices. In previous versions, you could only aggregate up to 5 Peregrine appliances.

If you are near the 50,000 device limit, an alarm will be displayed in **Status > Appliance Health**.

General UI improvements

There are a few general UI improvements:

- If you mouse over a device link in an HTML page, the IP address is shown in the status bar, if available.
- URL links to the assistant are underlined with a dashed line.
- If there is stale data, the information is displayed with a gray background. This works in the Health Panel, Alarms Viewer, and all the Managers.

Toolbar

All of the icons on the Main Toolbar and other product toolbars (Device Manager, Port Manager, Line Manager, etc.) have been redesigned.

There are new Main Toolbar buttons for the following features:

- Aggregate Alarms Viewer (only seen in Aggregator mode)
- Alarms Viewer
- MIB Browser
- Download

In an Aggregator, the list of “Remote Appliances” is now sorted by name instead of IP address.

All Applets

File Menu

When your appliance is in Aggregator mode, the **File** menu has an **Appliance** submenu for remote appliances.

There is a new command called **Connection Info** which replaces the **Session Info** command from previous versions of Network Discovery. This new command is available whether or not a map session is open. Also, the **Connection Info** command displays information on the User, Server, and Map Session.

Object Menu

There is a new **Update Model** submenu with the following commands: **Query Network**, **Upgrade Scanner**, **Run Scanner**, **Retrieve FSF**, and **Run Rulebase**. (**Upgrade Scanner**, **Run Scanner**, and **Retrieve FSF** are only available if using Network Discovery with Desktop Inventory).

There is a new **Visibility** submenu with the following commands: **Deactivate**, **Hide**, and **Purge**.

There is a new **Manage** submenu. In previous versions, the list of commands appeared in the **Object** menu.

Tools Menu

Icons have been added to the commands in the **Tools** menu.

Date formats

All applets use the user's preferred date formats as entered in **Administration > Account administration > Account properties**.

Network Map

There have been many changes to the Network Map:

Icons

- Some new device icons have been added, and many of the device and package icons have been redesigned.
- If a device has been deactivated, hidden, or purged, a red X will be placed over the icon until the end of the poll cycle at which time the icon will disappear from the map.
- When you change an icon, the change happens on the Network Map immediately (not at end of poll cycle, as in previous versions).
- Devices that are “not-seen” are displayed as pale images (rather than with gray icons or gray backgrounds, as in previous versions).

The Look of the Map

- When dragging a group of icons, the boundary and drag origin are displayed while dragging. The group can be easily moved back to the origin (snap into place) to prevent moving the object to the wrong location).
- Non-alarmed objects/lines are indicated by thin circles/lines.
- Alarmed objects/lines are indicated by thick circles/lines
- A device is never circled if the alarm cannot apply to it (even if it is within the minimum priority range).
- Devices (ports) generating line alarms are circled, and packages containing line alarms are also circled.
- The alarm colors have changed to match the alarm icons seen on the Health Panel and elsewhere in the product: Critical alarms are red, Major alarms are orange, Minor alarms are gold, and Info alarms are green.
- A “found” object is identified with a spotlight (a large pale yellow circle) rather than a magenta square.

Selected Objects

- A selected object has a darkened icon and gray text background.
- A selected line is highlighted with a dark outline.
- The selection marquis (dotted box when selecting a group of objects on the Network Map) disappears when selection is complete.

Commands and Buttons

- The **Reconnect** command closes all open map windows except the Main Map.
- A **Delete** button has been added to the **Save As** dialog.
- A **Find** button has been added to the map to find a device and highlight it.
- The **Object** menu has a new **Top of Network** command (which replaces the top-of-network property from previous versions.)
- There are new map scaling commands: **Scale to Fit Width** and **Scale To Fit Height** (these commands replace **Fit Map to Window** from previous versions).
- For printing, map tiles are represented by page numbers (rather than two-dimensional tile numbers) to conform to the new print dialog.
- New **Select All** command on the **Edit** menu

Pop-up information

- If a device has a ticket open in ServiceCenter for the currently selected alarm, the ticket number(s) appear in the pop-up.
- The pop-up information has header with icon.
- The line pop-up information includes line speed.

Alarms

- The Map supports new alarms (disk utilization, CPU utilization, backplane utilization, exceptions, etc.)
- Alarms updated in real time (not at end of poll cycle).

Lines

- A multiline appears as line of dashes.

Packages

- Tags for packages are displayed in bold blue font to distinguish them from devices.
- Tag color for “visited” packages changes to magenta.
- A New Package is positioned at right-click position.

New Control Bar

- The new control bar is at top of Map windows, and replaces the status bar which appeared at the bottom of Map windows.
- The control bar has controls to select alarm and priority range, select a user's map configuration file, rescale the map, and move up a level.
- The control bar displays package alarm state, mouse-over alarm state, scale, and number of devices in the package.

User preferences

- User preferences are visually demonstrated when selected.
- User scale preference can be any integer value between 1 and 300.
- There is a new “Arc” line style.
- There is a new preference for displaying full (untruncated) object titles on the map.
- There is a new preference for selecting alarm types to show on the Health Panel.

Technical





- Improved map rendering with Graphics2D (alpha, antialiasing).
- Continuous map scaling with AffineTransform.
- New accelerator keys and command mnemonics.
- Tool tips on all controls and text fields.
- Provides mouse-wheel support.

Health Panel

The Health Panel has been completely redesigned, with the following changes:

- There are six columns: alarm state, alarm name, plus counts for Critical, Major, Minor, and Info.
- There are new alarms seen on the Health Panel:
 - Frame Relay
 - Disk Utilization
 - CPU Utilization
 - Load Average
 - Memory Utilization
 - Backplane Utilization
 - Printer
 - UPS
 - Port MTTR
 - Port MTBF
 - Port Adds/Deletes
 - Port Moves
 - Port Changes
 - Device MTTR
 - Device MTBF
 - Device Adds/Deletes
 - Device Moves
 - Device Changes
 - Exceptions
 - Not Recently Seen
 - Open Tickets
- You can sort the information based on any of the columns.

- There are new icons to distinguish device and port alarms. In 5.1, the Health Panel is divided into 4 sections as indicated by these new icons, rather than by separator bars (as in previous versions).

Previous Versions	Version 5.1	Indicator
Line Fault	Port Attribute Alarm	
Device Fault	Device Attribute Alarm	
Metrics	Port Report Alarm	
	Device Report Alarm	

- Alarm state indicates highest alarm state having non-zero counts.
- The new control bar has options to select alarm and priority range, or open an Alarms Viewer for the current selection.
- The new appliance status bar (at the bottom of the Health Panel) contains an appliance report button, appliance alarm state and count, demo/forecast mode, server clock and communication status.
- The new View menu has commands to hide inactive alarms, display the user's preferred alarm set, refresh the display.
- When you close the Health Panel, and open it again, it appears where you last placed it on your screen. If the video resolution changes, the Health Panel location is adjusted accordingly.
- Network availability (as seen at the bottom of the Health Panel) is computed on priority 3 devices and up instead of priority 4 and up.

Alarms Viewer

In earlier releases, there were buttons on the Health Panel that would open “Health Panel reports.” In Network Discovery 5.1, the Alarms Viewer replaces the Health Panel reports.

Now, in a single window, you can now toggle between types of alarms to see the alarmed devices in the network.

Here are some significant features of the Alarms Viewer:

- **Edit > Copy** produces tab-separated values which will paste into Microsoft Excel with **Edit > Paste**.
- You can sort the information based on any of the columns.
- The control bar has options to select alarm and priority range, refresh the display, open the Device/Port Manager for the current selection, to find the current selection on the Network Map, or to show more information about the current selection.
- The control bar displays the number of alarms and highest alarm status.
- The Alarms Viewer is not automatically refreshed (manual refresh provided)
- Right-click support.
- The display is limited to 1000 items.

Exceptions Report

- The Exceptions report is now available through the Health Panel and Alarms Viewer (instead of through **Reports > Support > Exception Summary**, as in previous versions).
- Choose the “info” button on the Alarms Viewer for detailed description of the exceptions.

Service Analyzer

- The Service Analyzer has been redesigned, and converted into a Java applet. There are three panels in the Service Analyzer window:
 - Path Alarms
 - Path Graphs
 - Summary Graphs
- The path portion of the Path Alarms tab looks and works like the Network Map. The alarms portion looks and works like the Alarms Viewer.
- The path shown in the Service Analyzer is based on data from the last 48 hours. In previous releases, the time interval was “yesterday + today.” Using “the last 48 hours” consistently provides more data.
- All the graphs in the Service Analyzer have a consistent appearance.
- The availability graph has been removed. In its place, the summary graphs have been changed to display a lighter color where the displayed path was not active. To see this feature, find a path with a device that has been broken for part of the last 48 hours, and look on the graphs in the Summary Graphs tab.

Events Browser

The Events Browser has been completely redesigned, and converted into a Java applet. There are also the following changes:

- **Edit > Copy** in Events Browser produces tab-separated values which will paste into Microsoft Excel with **Edit > Paste**.
- An **Object** menu and right-click menu has been added.
- You can sort the information based on any of the columns.
- A new Find button opens Find dialog.
- The control bar has options for filtering events displayed, as well as buttons to open the Device Manager and Port Manager.

MIB Browser

- The MIB Browser has been completely redesigned to make navigation easier.
- There is a new Find button that opens the Find dialog.
- There is a pull-down list of recently selected devices.
- There is a new Variable tab available to perform Set operations.
- It now supports a “folder” view of the MIB, where the contents of all children of a MIB node are read and displayed simultaneously.
- There is a new refresh button.

Find

The Find feature will automatically locate the device on the Network Map, if the map is open.

The Managers

There are some changes common to the Device Manager, Port Manager, and Attribute Manager:

Statistics

- There is now support for graphing predictions. You can see a prediction for 30, 60, 90, 180, and 360 days into the future.
- New Y-axis maximum option of “Forecast”.
- Thresholds are now shown as intervals on the left y-axis rather than just as horizontal lines. Symbols indicating the alarms are also shown.
- Changed y-axis scale for attributes that are time-based so it reads as weeks/days/hours/minutes/seconds as appropriate.
- Show “changes” graph for “Pages Printed” attribute.
- New option to allow you to draw or not draw the thresholds on the graphs.

Text

- In previous versions, you had to reselect the original Device Manager button to leave the “text-only” panel. In 5.1, you can click the Text button again and see the original panel.

Events

- The Events button (on Device Manager and Port Manager) now opens the Events Browser, which will list events only on the one device or port.

Device Manager

There have been some changes to the Device Manager:

General

- The order of the buttons on the toolbar has been changed.
- The Device Manager now shows information when the device is deactivated or hidden.

Configuration

- A “Hardware Manufacturer” field has been added.

State

- There are more Attributes listed. For a full list of attributes for version 5.1, see [Help > Classifications > Supported Device/Port Attributes](#).

Reports

This is a new panel in 5.1.

There are three sections:




- State
 - Shows all Report information from Alarms Viewer.
 - Exceptions are listed here (moved from the Configuration panel).
- Metrics
 - There are new Metrics values for data points in the time period: Mean, Mean Peak, Peak, Peak Time, Mean Minimum, Minimum, and Minimum Time.
- Events
 - Summarizes events for Yesterday, Last 7 Days, Last Week, Last Month, and This Month.

Diagnosis

- The “Device Management” table has been removed, and the data has been merged into the first table.
- There is a new “Listener Ping” button.

Ports

- There are links for each statistic that is shown, linking to the Attribute Manager.
- The statistics now match exactly what is in the Port Manager.
- In earlier releases, round parentheses would appear to indicate that the value is not from the past poll cycle. This is no longer the case. A grey background is used consistently when the statistics are older than the user-defined threshold.
- There are new icons for port status.

Previous Version	Version 5.1	Meaning
green circle		OK
gray circle		unknown
red circle		broken

Update Model

- In previous versions, there was only one option: updating the device model.
- In 5.1, there are 5 “Update” options:
 - Network (which is the same as the old “Update Model” function)
 - Upgrade Scanner
 - Run Scanner
 - Retrieve FSF
 - Rulebase

Note: Upgrade Scanner, Run Scanner, and Retrieve FSF are only available with Desktop Inventory awareness.

Device Visibility

- In previous versions, there was only a **Purge Device** button.
- In 5.1, there are 4 “Visibility” options:
 - Activate
 - Deactivate
 - Hide
 - Purge

Properties

- You can access the Properties dialog from the Device Manager even when in inventory-only mode.

Port Manager

There have been some changes to the Port Manager:

Configuration

- An MTU (Maximum Transmission Unit) property has been added.

Reports

- This is a new panel in 5.1.
- There are new Metrics values for data points in the time period: Mean, Mean Peak, Peak, Peak Time, Mean Minimum, Minimum, and Minimum Time.

Diagnosis

- The “Port Management” table has been removed, and the data has been merged into the first table.
- There is a new “Property Assignment” table.

Properties

- This is a new button in 5.1. Clicking the **Properties** button will open the new consolidated Port Properties dialog, which replaces the **Interface Rate**, **Interface Type**, **Alarm Type**, and **Duplex Mode** buttons from previous versions.

Attribute Manager

There have been some changes to the Attribute Manager:

- Forecast information for an attribute is visible.
- Both the default and user-assigned thresholds are visible.
- On the Attribute Manager State panel, there is a new “State time” that indicates when Network Discovery changed the state. “State time” is a new field. Upon upgrade, State time will be set to the current time. It will update with the state change thereafter.
- Disk serial number and disk volume label are now stored for SNMP managed MS windows servers/workstations as separate properties rather than being rolled into the attribute description

Administration Menus

The Administration menus have been streamlined, improving navigation through the product.

The inline help on the Administration pages has been improved.

There are more features with “reset to defaults” options.

Basic Administration

Appliance Management

There is a new **Install License** option to allow licences to be installed through the HTML UI. The traditional way of installing licences via the share is still supported.

Account Administration

There is a new preference in the Account Administration menu: **Minimum Password Length**. The Network Discovery Administrator can set a minimum length for all account passwords.

There is a new feature in the list of account properties: **Password Expiry**. The Administrator can set how long an individual account can go unused before the password expires.

Network Discovery will warn you if your password is going to expire in the next 7 days. When you login, there will be a warning message at the top of the Home Page.

Network Configuration

There are two new options: Scanner Property Groups and Listener Property Groups. These are only available in Desktop Inventory awareness-mode, and help you work with both products.

Notification and Events Configuration

ServiceCenter Configuration

This is a new menu in Network Discovery 5.1.

Event Filter Configuration

You can now delay notification of events (e-mail, pager message, SNMP trap, ServiceCenter ticket). This feature was created so events that when events are corrected automatically within the set delay period, no notification will occur.

Notification possible on more items

- all thresholdable attributes
- property and connection events
- delayed notification ability.
- new notification type (ServiceCenter)

Logging is enabled all the time (all events are logged).

Note: Upon upgrade/migration, event filters which only have log as the type will be removed.

Advanced Administration

This menu has been redesigned, and several new features have been added to make Network Discovery administration easier.

System Preferences

The old **Network Tuning**, **Appliance Services**, **Display Preferences**, and **Device Manager Ports Display Preferences** menus have all been combined in a new menu called **System Preferences**.

Many new configuration options have been added as well.

Automatic Packaging

Automatic packaging is based on connectivity, not on icon (as it was in previous releases). There are a few basic scenarios:

- device with one connection, to a single NCD
- device with multiple connections to a single NCD
- devices connected to a cloud or phone, which has a single connection to an NCD (in this case, the cloud or phone is also packaged with the devices).

Schedule Management

This is a new feature in Network Discovery 5.1. It will only be available if you are using Desktop Inventory with Network Discovery.

Data Management

There are some new options in this menu:

- Update network model in cases where the normal update network model in the device manager does not work.
- Force Database checkpoint
- Erase all tickets

The following will only appear if you are using Network Discovery with Desktop Inventory:

- Validate Scanner Configuration
- Manage Scanner Configuration
- Validate SAI
- Manage SAI

Router Discovery

The list of community strings to use for router discovery is now a configuration option in router discovery. Previously router discovery used the community string list in from network configuration.

Status

Appliance Health

Monitors many new things such as:

- Scan File Processing
- Mail Queue Status
- Sampling Period

Hardware Environment

There are a few new items on this page:

- Modem status
 - shows presence of a modem
 - detects if it is compatible with rest of system

Software Environment

There are a few new items on this page:

- Licence Capacity Utilization - now displays aggregation licence info
- Aggregation - warns if any appliances to be aggregated are unreachable
- Network Discovery Info - Displays factors affecting discovery when having abnormal values
 - table reader drop rate
 - device modeler queue size and time of oldest request
- Notification Queue Status - Size of each of the notification queues (and timestamp of oldest message if applicable) is displayed

Device Model Status

Modeling status now shows the list of devices currently being modelled queue as well as those that are pending.

Icons for devices in the queue are shown where possible. All devices can be clicked to open the Device Manager.

Current Settings

Expanded to show all the new system preferences and thresholds.

Filtered Devices

If a new device is added to the database, some records referring to it are removed from the list of filtered devices.

There is a new filter item for list of devices which are responding from a different IP address from which they were pinged by the Network Explorer.

There is a new filter item for when trying to re-activate a device, but there is insufficient licence capacity to do so.

Active Devices

Replaces the previous report: **Reports > Support > Device Inventory Export**.

Deactivated Devices:

This is a new list.

Hidden Devices

This is a new list.

Forced Connections:

There have been some formatting changes to make it more readable.

Reports

Move the Aggregate Summary Reports up one level under Executive/Summary Network Reports on the main Report menu.

Clean up all performance with bar graphs so that bars are aligned with graph value.

Add Current Month period to all performance reports.

Packaging information added to all device reports.

Added new Top Talkers and Top Listeners reports: lists end node devices with highest average “in bytes” and “out bytes” values, respectively.

Download

There are new items in the Download directory:

- Peregrine Trap MIB
- Registry file to enable Desktop Inventory to be aware of Network Discovery.
- Java Runtime Engine 1.4.2 (the file is called “j2re-1_4_2-windows-i586.exe”).

The following components of Desktop Administration are for use with Desktop Inventory awareness:

- agents for windows, aix, solaris, hp/ux, linux
- quick deploy console

Help

There are new items in the Help menu:

- New classification documentation for:
 - Device Categories
 - Interface Types
 - Line Alarm Types
 - Package Alarm Types
 - Alarms
- Under Classifications, the Device/Port Attributes have been extended to show more information
- New Database Schema documentation

Device and Port properties

You can now change device/port properties without having the Network Map open. Also, you can have multiple properties dialogs open simultaneously.

Port Properties

There is a new consolidated Port Properties dialog.

You can now configure the line speed up to 1Tb/sec.

Device Properties

When you change the icon, the priority is no longer automatically changed.

Device properties are now changed per-user rather than per-user-per-map (i.e. only one set of device properties per user). In earlier releases, you could have different device properties in each of your map configurations. This is no longer the case. When migrating/upgrading, the last map configuration used is used for the user-assigned properties.

Administrator and IT Manager accounts can now change system-level properties. These system-level properties can effect all users. They can change:

- Icon
- Tag
- Title
- Priority

When migrating/upgrading, the initial system title and priority are taken from the title and priority in the 'Prime' configuration.

When device properties update, they are now immediately visible on the Network Map and in the Device Manager (in previous releases, that would happen 30 seconds later).

All accounts can now change device titles and priorities for their own account with “My User Properties.” These user properties do not effect any other accounts.

The Properties dialog no longer shows Top-of-Network property (replaced by Top of Network command on Object menu).

Alarm Threshold Defaults

The Alarm Thresholds dialog has been redesigned.

In previous releases, you had to reset all the thresholds to defaults at once. In Network Discovery 5.1, you can reset alarm thresholds to defaults on a threshold by threshold basis.

There are a few new features:

- **Copy and Paste** feature in the Alarm Thresholds dialog. This allows you to duplicate thresholds for different types of alarms.
- You can set the thresholds to n/a by choosing the “Custom” radio button and clicking **Apply**. This allows you to turn off alarms that are generated by default.
- Thresholds can range up to positive infinity. Use the “+” (plus sign) to indicate this.

Note: Thresholds are applied when the next value is received.

Forecast

The forecast feature has been improved. The forecast time periods available have been reduced to 1, 2, 3, 6, 9, and 12 months.

The Health Panel now shows only relevant alarm categories. Non-forecasted alarm categories will not appear. Forecast information is also available in the Attribute Manager.

Forecast data is only generated if there are at least 21 days of data for that attribute. You can see a list of the forecasted attributes by clicking **Help > Classifications > Supported Device/Port attributes**.

Note: Aggregate windows do not support forecast mode

Deactivation

In earlier releases, there were two steps to have a device removed from the Network Discovery database: trash and purge. In 5.1, the term “deactivate” replaces the term “trash.”

At the end of the deactivation interval, the device become inactive. The device will appear in a list of deactivated devices, and waits to be either purged, or manually reactivated.

There continues to be a 10% limit of devices that have been deactivated. When Network Discovery is over this limit, it will automatically purge devices.

Hidden Devices

This is a new concept in Network Discovery 5.1. Instead of purging a device on your network (and risking its return to the Network Map when Network Discovery discovers the device again), you can “hide” a device.

By making a device hidden, it will never appear on the Network Map, and Network Discovery will not gather any statistics about the device.

Hidden devices contribute to your license count.

Reactivation

This is a new concept in Network Discovery 5.1. If a device has been deactivated or hidden, you can “reactivate” the device so it will appear on the Network Map and in Network Discovery reports.

Note: A reactivated device will only appear in current reports as they are generated.

Database Schema

The Database Scheme is now fully documented online. See [Help > Database Schema](#).

Changes to the Database Schema since Network Discovery 5.0 are as follows.

In Network Discovery 5.1, the contents (and meaning) of the Event table have been completely changed.

The following tables have been added:

- Attribute
- AttributeState
- AttributeGroup
- DeviceIcon
- EventSummary
- hwAssetAnalysis
- hwAssetAutomatic
- hwCMOSMemory
- hwDOSGroup
- hwNetworkAppleTalk
- hwNetworkIpx
- hwNetworkNIS
- hwNetworkNames
- hwNetworkNetbios
- hwNetworkTcpip
- hwOSClusterInfo
- hwOSClusterNodes
- hwOSLocaleData
- hwOSStandardWindowsDirectories
- hwOSWallPaper
- hwOSWebBrowser
- hwPartitionData
- hwRecognitionInfo
- hwUnixSystemConf
- hwUserData
- hwVirtualMachine
- hwsmbiosBIOSLanguageInformation

- hwDOSMemoryData ■ hwOSMailClient ■ hwsmbiosCacheConfiguration
- hwLegacyFPUData ■ hwOSScreenSaver ■ ReportState
- hwMountPointScanData ■ hwOSShell ■ ReportDetail

The following tables have been removed:

- Alarm ■ ExceptionCategory ■ hwIPAddress
- DeviceExtension ■ Health ■ Metric
- Exception ■ hwDNS

The following fields have been removed from existing tables:

- Device.DeviceCategory_IDPreferred ■ Port.Port_Index
- Device.Device_DefaultPriority ■ Port.Port_SpeedIn
- Device.Device_AddedToMapDt ■ Port.Port_SpeedOut
- Device.Device_PriorityLabel ■ Port.Port_PreferredMACAddress
- DeviceCategory.DeviceCategory_GraphicFileName ■ Port_Status
- DeviceCategory.DeviceCategory_NetworkClassification ■ Port.Port_FirstFoundDt
- DeviceCategory.DeviceCategory_FunctionClassification ■ Port.Port_PreferredIPAddress
- DeviceCategory.DeviceCategory_DefaultPriority ■ Port.Port_AddedToMapDt
- DeviceCategory.DeviceCategory_IconSortOrder
- DeviceCategory.DeviceCategory_GroupID
- DeviceCategory.DeviceCategory_IconDescription

The following fields have been added to existing tables:

- Appliance.Appliance_HTTPReturnCode ■ Device.Device_SerialNumber
- Device.DeviceIcon_ID ■ Device.Device_PreferredDNSName
- Device.Device_PkgLabel ■ Connection.Connection_LastChangedDt
- Device.Device_FullyQualifiedLabel

Internal improvements

Appliance changes

Modem Driver

The modem driver for the Buffalo/Melco modem used in the IBM x335 server was updated to a newer revision. Changes were made to the way modem detection is handled and the country code was set.

UPS

A fix for Japanese late model APC USB UPS systems was installed, allowing for more compatibility with various UPS models.

DNS Resolution

The way that DNS resolution is done on the appliance was changed, allowing for local caching of DNS responses and increased compatibility with Microsoft DNS servers.

No longer changing MAC address

In previous releases, Network Discovery would change the MAC address of your Peregrine appliance. Starting in version 5.1, the manufacturer's MAC address will remain unchanged. (i.e., your IBM server will revert to its IBM MAC address.)

RAM

The Peregrine appliance now supports two new memory sizes: 2.5 and 4GB. The maximum number of devices is still 10,000.

CPU

Dual-processor x335 servers are now supported.

Network Explorer

The minimum discovery interval has changed from 2 minutes to 10 minutes to avoid extra pinging of devices when the discovery range is small.

To speed up initial discovery: the broadcast address of the local segment is now the first address in the list (if it is in the IP range).

When the Explorer has detected that it has pinged a broadcast address, that IP address is put on a block list for 7 days.

Device modelling

Modelling Phases

Device modelling now has 3 distinct phases:

- Network
- Scan; which is made of these sub-phases
 - Upgrade scanner
 - Run scanner
 - Retrieve FSF
 - Enrich with XML Enricher
- Rulebase

Whenever the Network or Scan part of the device model changes, the rulebase is automatically re-run. The rulebase part of the device model is also automatically run when:

- the rulebase is upgraded
- there is a change in **Administration > System Preferences > Display Preferences > Device Title Preference**

These automatic updates are scheduled to run at a lower priority. You can also manually re-run the rulebase portion of the device model to avoid waiting for the automatic updates to run, which may take up to an hour.

Rulebase model update will recalculate the following:

- Model
- Family
- Operating system

- Network function
- Manufacturer
- Title
- Tag
- Priority
- Icon

Model Updates

If the model received from the network is a MAC-only, it will not update an existing device model which is IP+MAC or SNMP managed. This prevents stale IP+MAC pair from being kept around longer than it would be normally.

Environmental poller

The Environmental poller is used to poll attributes at very low frequencies, by default once per day. Unlike the other Network Discovery pollers, if the attribute cannot be retrieved, polling will be re-tried (by default every 2 hours).

Environmental attributes are subject to the same restrictions as the Resource attributes:

- There must be enough resource/environment licenses
- Device must be in the resource/environment IPv4 range in **Administration > Network Configuration**.

The Environmental Poller can be disabled in **Administration > System Preferences > Appliance Services**.

The Environmental Poller Rate, Retry Interval and Retry Count can be changed at **Administration > System Preferences > Network Devices**.

The toner level attributes in printers have been converted from the Resource poller to the Environmental poller to reduce the SNMP load placed on printers.

Table reader

Diagnostic Information

The list of Table Protocol details in the diagnostics panel of the Device Manager and Port Manager has now been expanded. The list is now:

- ARP table (device level and port level)
- Bridge table
- Source Address capture
- Radio link
- Bus link
- Carrier link
- Link training
- Detailed link training

The time a protocol was last seen is recorded and visible, and updated every 30 minutes.

The protocol will still be seen even if all the addresses seen by the protocol handler are filtered. This will clear up false exceptions.

Table reader rate controls

If table reader reads more table entries than the system can handle, the table entries are buffered and sent at a slower rate to avoid making the system become unavailable.

Persistence of this condition will lead to an alarm in Appliance Health. You should notify customer support and lower the table reader rate if this occurs.

Broadcasts

In earlier releases, there was on a “Broadcast Warning” threshold. When Network Discovery determined that a port was the source of the broadcasts, it would change the warning to an alarm. Broadcast warnings did not generate events, while broadcast alarms did.

This behavior is now changed so that “Broadcasts In” and “Broadcasts Out” have the full range of thresholds available. When the system determines that a port is the source of broadcasts, the “Broadcasts Out” counter is copied into the “Source of Broadcast” counter for the port. “Broadcasts In” and “Broadcasts Out” do not generate events, “Source of Broadcast” does.

Virtual device handling

Virtual device creation now works more reliably so that when a new virtual device is created, its title is immediately visible in the database and on the map, rather than one poll cycle following its creation.

Notification of creation and deletion of new virtual devices works more reliably.

Break handling

Devices can no longer be in a Break state for the first 24 hours of existence. For the first 24 hours, the break state will be “n/a.”

Also, “Total Breaks” and “Downtime” are not computed for the first 24 hours.

Alarm Reports

Unlike Attributes which are updated as data is collected from the network, reports are updated less often. The following table lists how often these reports are updated:

Report	How often it is updated
Device/Port Add	15-20 minutes
Device/Port Delete	15-20 minutes
Device/Port Move	15-20 minutes
Device/Port Change	15-20 minutes
Device Not Seen	15-20 minutes
Open Tickets	15-20 minutes
Exceptions	30-60 minutes
Device/Port MTTR	daily
Device/Port MTBF	daily

Ports License

The Network Discovery ports license is equal to 6 times the number of devices, unlike in previous versions, where there was a limit of 45,000.

New Line Alarm Types

The following new line alarm types have been added:

- user defined 3
- user defined 4
- user defined 5
- backplane

Updated device scripts

The device scripts have been updated to handle additional devices with non-standard SNMP MIBs, or better handling of existing ones. This improves the ability to model the devices in your network accurately and determine how they are physically connected.

Updated device rulebase

The device rulebase has been updated with the latest information about vendors and models of devices so that the devices in your network are accurately identified.

Miscellaneous

- MySQL upgraded to the latest version 3 release.
- Apache upgraded to latest release.

Upgrade/Migration information

The upgrade information is in the following sections:

- *Upgrading from Peregrine's Network Discovery 5.0, 5.0.1, or 5.0.2* on page 42
- *Migrating from InfraTools Network Discovery 4.2 or 4.3* on page 43
- *Migrating from Xanadu* on page 43
- *After an upgrade* on page 43

Warning: The procedure for upgrading/migrating varies depending on what version of software you are currently running because the platforms differ. If you are in any doubt, check what version you have.

To check the version of Network Discovery you are currently running

- ▶ See the version number at the bottom of the Toolbar.

If you have more than one appliance, check which version of Network Discovery is running on *each* appliance. Follow the correct upgrade/migration path for each appliance separately.

Note: Migrating from ND 4.1.1 or earlier is not supported. If you have an older appliance you must upgrade in steps, from one release to another. (You may be able to skip releases between your earlier version and version 4.0. To find out, contact Peregrine Systems Customer Support.)

Upgrading from Peregrine's Network Discovery 5.0, 5.0.1, or 5.0.2

If you are upgrading your appliance from Network Discovery 5.0/5.0.1/5.0.2 to Network Discovery 5.1, follow this procedure.

Before the upgrade

Before you perform the upgrade, check that you are still entitled to customer support. The Network Discovery CD will not work if the appliance is out of maintenance.

To check that you are still entitled to support

- 1 Clicks **Status > Current Settings > Installed Licenses**.
- 2 Check the entry, "Maintenance valid until".

If your Maintenance license has expired, renew the contract and contact Peregrine Systems Customer Support for an updated license key.

If you are using Aggregation

- Check that each remote appliance is running 5.1 or later. If not, the Aggregator appliance will not read the remote appliance's data.
- check the maintenance date for each Peregrine appliance.
- Always upgrade the Aggregator appliance *first*.

Performing the upgrade

Note: You can use a monitor and PS2 keyboard attached to the Peregrine appliance or you can use the management workstation to restart the Peregrine appliance through the browser interface at **Administration > Appliance Management > Appliance Restart**.

To upgrade Network Discovery software

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

The system then reboots from the CD. The CD does not overwrite any newer software components that you have downloaded from the Customer Support web site. After the components have been installed, the CD ejects, and the server reboots.

- 2 Remove the CD, and store it in its case in a safe place.
Network Discovery is now upgraded to version 5.1.
- 3 If you are using a monitor attached to the Peregrine appliance, press **Enter**.

The monitor shows **Password:**. If you are using the web browser at the management workstation, Network Discovery comes back on.

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

Migrating from InfraTools Network Discovery 4.2 or 4.3

Essentially, the process is to take a backup from your old appliance and restore it onto the new one. The instructions are in the *Setup Guide*.

You no longer need to enable firewall ports 2120/tcp, 2121/tcp or 2323/tcp. Refer to the *Setup Guide* to see what ports must be enabled.

Migrating from Xanadu

Xanadu uses an IBM xSeries 330 server. The procedure to migrate it to Network Discovery 5.1 is to take a backup from the Xanadu appliance, install the new software onto the IBM xSeries 330 (or a new xSeries 335) server and then restore the backed up Xanadu data onto the Network Discovery 5.1 appliance. The instructions are in the *Setup Guide*.

After an upgrade

It's a good idea to check you have the latest software components from support.peregrine.com. There are instructions for checking and installing software components in the *Setup Guide*.

Documentation

There are new updated versions of the Network Discovery *User Guide*, *Data Export Guide*, *Setup Guide*, and *Reference Manual*.

There is a new manual: *Using Network Discovery with Desktop Inventory*.

For a complete list of current Network Discovery documentation, see the Documentation pages on the Peregrine Customer Support web site at <http://support.peregrine.com>. (Access to this web page requires a current login name and password.)

You can download documentation PDF files and view them using Acrobat Reader, which is available on the Customer Support web site and through Adobe at <http://www.adobe.com>.

Dropped functionality

The following items have been removed from Network Discovery 5.1.

- NEWS. With the improved Forecast functionality, NEWS was no longer needed.
- Purging several devices from the Map at once. Devices need to be purged one at a time.
- Reset MTTR/MTBF has been replaced by MTTR and MTBF time periods in **Administration > System Preferences > Report Time Periods**.
- Support for browser's internal JVM (requires Java Plugin instead).
- Displaying device alarms and line alarms simultaneously on the map (only one alarm can be displayed at a time).
- Line thickness on the map no longer indicates line speed (it identifies an alarmed line instead in support of accessibility requirements, line speed is displayed in popup info).
- On the Network Map, the **Object > Open** command is no longer available when multiple objects are selected on the map (you must select a single object to open it).
- The Map window does not indicate the number of objects in the package, though it still indicates the number of devices contained recursively within the package.
- The Map window has no clock (it is now on the Health Panel).
- The Map window has no button to access the Health Panel (still accessible via the Health Panel command on the Tools menu)
- The Map window and Health Panel have no progress meter to monitor the poll cycle (alarms are now updated in real time).
- There are no user preferences for alarm colors (alarm states are distinguished visually by icon shape, as well as by color, to meet accessibility requirements).
- There is no user preference for displaying only outlines of icons when dragging them on the map.

- There is no user preference for how to display selected objects on the map (selected object always has a darkened icon plus gray text background).
- No longer display port indices in end node packages.
- The IND 4 XML for integration with Connect-It is no longer supported. Connect-It 3.3 introduces a new connector. The generic ODBC database connector can also be used.

Known issues

Workgroup

In some cases, the appliance will not show up in the Windows “network neighborhood” using the configured workgroup. It may not show up at all.

Use the IP address of the appliance to access the share.

Aggregator setup

When you add multiple remote appliances that have populated data, do not add them all within the same day. Wait at least 24 hours between adding each appliance.

Time zone change after restore

If a backup contains a time zone different from the time zone on the appliance, restart the appliance after restoring the backup. Alternatively, change the time zone of the appliance to the time zone of the backup before you do the restore.

Some tape drives do not work

There are some USB tape drives that do not work with the Peregrine appliance.

New Data for some New Interface Elements

Many of the new user interface elements require new data to be collected. If you're migrating from 4.2/4.3 or upgrading from 5.0, you may find some data elements missing or incorrect until such time as either

- two poll cycles have passed
 - state of the attribute in the Device Manager, Port Manager, and Attribute Manager.
- the device model is updated

- priority of deactivated devices
- title of deactivated devices
- icon of deactivate devices
- the attribute state changes
 - the 'time since' shown in the mouse-over of the attribute state icon shows the time of the upgrade, not the time of the state change.
- the aggregate database updated
 - empty columns in the database including Package and FullyQualifiedPackage

Note: Please let your new version run at least 24 hours before reporting problems to Customer Support.

Time of Adds/Not Recently Seen/Moves

If migrating/upgrading to 5.1, the time for your Add/Not Recently Seen/Move events are not preserved. Set the new value in **Administration > System Preferences > Report Time Periods**.

Upgrading with an Aggregator

The aggregator is not compatible with versions previous to 5.1. Upgrade the aggregator first then all the other appliances in quick succession.

Due to the database changes, please let your new version run at least 24 hours to catch up on missing data before reporting problems to Customer Support.

Hardware Upgrade every 2-3 years

Every new major and minor release of Network Discovery adds new features, extending the software functionality to meet our customers' needs. These additional enhancements may introduce new demands on the original hardware, subsequently impacting performance. Customers employing older platforms may find that this release performs a little more slowly than the previous release. Customers should be prepared to upgrade their Network Discovery appliance every 2-3 years to maintain optimal performance, as they would other enterprise application servers.

Unix Listeners

In *Using Network Discovery with Desktop Inventory* (chapter 2) and *User Guide* (chapter 19), there are descriptions of how to install and use UNIX listeners. This function is not supported in Network Discovery 5.1.

Corrected issues

The following table contains corrected issues from the previous release of Network Discovery. For further updates see the Customer Support web site at <http://support.peregrine.com>.

What's affected	Description
Device Poller	Fixed handling of 64bit counters.
Device Poller	Sometimes if there were two device representing the appliance in the database, the poller would choose the wrong one, resulting in the map not updating.
Administration > Network configuration and Reports > Performance Summaries	The IP range diagram and summary graphs would not show properly when viewing via an aggregator.
Administration > IND 4 Network Configuration	Sometimes there would be no response from the web server when pressing the shift up and shift down buttons in Community Strings . This is fixed.
Table reader	The arp table was not filtered for invalid MAC addresses when read from the appliance. This is fixed.
Port Manager > Create Connection	You can now create a connection on a port immediately after breaking the connection. Previously you had to wait up to 48 hours before the port could be manually connected to another.
Historical Graph Data	Sometimes 0 (zero) values would be stored in the historical graphs when the attribute was not available. Now no value is stored, resulting in proper grey areas.
Event Summaries	Corrected the problem where in/out data would be merged together resulting in the problem state lasting longer than the reporting period. Upon migration/upgrade, all calculations of new reports ignore the old event summaries. Summaries are re-created for the 7 days preceding the upgrade. To have the reports reflected accurately, upgrade during the first 7 days of the month.

Need more help?

Peregrine is committed to ensuring your success with our products. We offer a number of ways for you to provide product feedback, suggest enhancements, and receive technical assistance with any issues you encounter.

For further information and assistance contact Peregrine's CenterPoint Web Site.

Peregrine's CenterPoint Web Site

Current details of local 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.



July 18, 2003